IIR

Internet
Infrastructure
Review

Mar.2023
Vol.58

定期観測レポート

SOCレポート

フォーカス・リサーチ(1)

データセンターと電力市場の関わり

フォーカス・リサーチ(2)

新設「IIJ Studio TOKYO」将来への架け橋

フォーカス・リサーチ(3)

IIJバックボーン30年間の変遷

IIJ
Internet Initiative Japan

Internet Infrastructure Review

March 2023 Vol.58

エグゼクティブサマリ …… 3

1. 定期観測レポート …… 4
1.1 はじめに …… 4
1.2 2022年セキュリティサマリ …… 4
1.3 セキュリティトピックス …… 7
1.3.1 2022年のEmotet …… 7
1.3.2 企業ネットワークへの侵入契機となるVPN機器の脆弱性 …… 9
1.3.3 2022年の脆弱性 …… 12
1.4 おわりに …… 17

2. フォーカス・リサーチ(1) …… 18
2.1 はじめに:電力市場とデータセンター …… 18
2.2 電力市場の課題1:電力コスト …… 18
2.3 電力市場の課題2:カーボンニュートラル(省エネと再エネ) …… 18
2.4 電力市場の課題3:新市場創設による電力安定供給 …… 23
2.5 最後に …… 25

3. フォーカス・リサーチ(2) …… 26
3.1 はじめに …… 26
3.2 IIJ Studio TOKYO 設備の概要 …… 26
3.3 なぜIPなのか?映像業界の課題とIPのメリット …… 30
3.4 NDI(Network Device Interface)のメリット …… 31
3.5 将来の映像制作 …… 32
3.6 過去の実績や取り組み …… 33
3.7 「IIJ Studio TOKYO」構築時の苦労した点や工夫 …… 35
3.8 後書 …… 35

4. フォーカス・リサーチ(3) …… 36
4.1 はじめに …… 36
4.2 IIJバックボーンの変遷 …… 36
4.2.1 1993 ~ 2002年 黎明期(リソース不足との戦い) …… 36
4.2.2 2003 ~ 2006年 普及期(品質向上とIPv6展開) …… 39
4.2.3 2007 ~ 2010年 トラフィック格闘期(BF化) …… 40
4.2.4 2011年~ネットワーククラウド(統合コアの構築と閉域の拡充) …… 42
4.3 IIJ ネットワークのセキュリティ対策 …… 43
4.3.1 Source Address Validation(送信元検証) …… 43
4.3.2 Internet Routing Registry(IRR) …… 44
4.3.3 Resource Public Key Infrastructure(RPKI) …… 44
4.3.4 Mutually Agreed Norms for Routing Security(MANRS) …… 45

Information …… 46

エグゼクティブサマリ

2022年11月にOpenAIから公開されたChatGPTが大きな反響を呼んでいます。ChatGPTは、名前から推測できるようにチャットボットの一種であり、チャットボットは従来から多くのシーンで利用されています。ただ、ChatGPTは、幅広い分野の質問に対して自然な受け答えができる、過去の会話を記憶している、作文やプログラミングができるなど、従来のチャットボットに比べて高度な能力を持っていることで注目されています。

筆者も試用したところ、先に挙げた特徴はまさにそのとおりで、驚くばかりでした。知らない事柄を調べる際には、検索エンジンから始めるのが一般的ではありますが、ChatGPTに質問を投げ、その回答を更に深堀して質問していくことで、検索エンジンを用いた調査よりも効率的に結果が得られるのではないかと感じました。ChatGPTが時には平然と誤った回答をするとの指摘はありますが、検索エンジンでも誤った情報が提示されることはあり、受け取った情報の真偽を見極める能力が要求されるという点は、従来と変わりないと思います。

インターネットに溢れる膨大な情報を整理して、必要なものにアクセスしやすくするという役割は、長らく検索エンジンが担ってきました。その裏ではAIが使われていたものの、利用者のインタフェースがAIチャットになり、必要な情報の要約まで含めてAIで処理されるというのは新鮮です。既にインタフェースをチャットにして、OpenAIのGPT-4を利用する検索エンジンも出てきており、長らく続いたユーザのインターネットにおける情報収集の体験が変わるのではないかという可能性を感じます。

「IIR」は、IIJで研究・開発している幅広い技術を紹介しており、日々のサービス運用から得られる各種データをまとめた「定期観測レポート」と、特定テーマを掘り下げた「フォーカス・リサーチ」から構成されます。

1章の定期観測レポートは、SOCレポートです。IIJのSOCでは、自社のサービスを運営することから得られる情報に加え、独自で収集している情報、社外から得られた情報の分析を行っています。本レポートにおいては、2022年におけるセキュリティの主要なトピックを振り返ると共に、その中でIIJのセキュリティアナリストが注目したEmotet、VPN機器の脆弱性に加えて、SOCで多く観測された4つの脆弱性について解説します。

2章のフォーカス・リサーチでは、情報通信産業に欠かせない電力を取り上げました。情報通信技術の発展に伴い、データの通信量・処理量が急増する中、環境保護の観点から電力使用量の抑制が強く求められることは言うまでもありません。日本における電力市場の課題と、データセンターを運営する電力の需要家としてのIIJの取り組みを説明します。

3章のフォーカス・リサーチでは、IIJの配信センターである「IIJ Studio TOKYO」の紹介と、そこで使われている技術を解説します。ネットワークと端末の進化により、様々な場面で動画配信が活用されるようになりました。映像業界と情報通信業界が交わるのが、インターネットの動画配信です。IIJ Studio TOKYOを含むIIJの映像配信のチャレンジについてご紹介したいと思います。

4章のフォーカス・リサーチは、IIJの創業30周年に合わせて、事業の根幹となるバックボーンネットワークの変遷を紹介します。IIJの創業以来、インターネットは拡大し続けており、IIJのネットワークも規模が大きくなるだけでなく、可用性・品質・セキュリティへの要求も格段に高まっています。それらに対して、IIJがネットワークをどのように進化させてきたのか、その記録を「IIR」に残すこととしました。

IIJは、このような活動を通してインターネットの安定性を維持しながら、日々、改善・発展させていく努力を行っています。今後も企業活動のインフラとして最大限にご活用いただけるよう、様々なサービスやソリューションを提供し続けてまいります。

島上 純一（しまがみ じゅんいち）

IIJ 取締役 CTO。インターネットに魅かれて、1996年9月にIIJ入社。IIJが主導したアジア域内ネットワークA-BoneやIIJのバックボーンネットワークの設計、構築に従事した後、IIJのネットワークサービスを統括。2015年よりCTOとしてネットワーク、クラウド、セキュリティなど技術全般を統括。2017年4月にテレコムサービス協会MVNO委員会の委員長に就任。

SOCレポート

1.1 はじめに

IIJではセキュリティブランド「wizSafe(ウィズセーフ)」を立ち上げ、お客様が安全にインターネットを利用できる社会の実現に向けて日々活動しています。SOCでは、wizSafe Security Signal[*1]を通じてセキュリティに関する情報発信や、IIJサービスの様々なログを集約している情報分析基盤を活用して脅威情報の分析を行っています。

本レポートは2022年におけるセキュリティの主要なトピックについて第1.2節で振り返り、取り上げたトピックに関連する脅威について情報分析基盤上で観測したものを中心に第1.3節で紹介します。

1.2 2022年セキュリティサマリ

2022年に話題となった主要なセキュリティに関するインシデントの中から、SOCが注目したものを表-1、表-2にまとめます。

＊1　wizSafe Security Signal(https://wizsafe.iij.ad.jp/)。

表-1 インシデントカレンダー（1月～5月）

月	概要・URL
1月	ソフトウェア開発会社は2021年12月31日未明にランサムウェアに感染したことを公表した。今回の攻撃ではファイルの暗号化だけではなく、顧客取引情報などのデータが攻撃者に窃取され、リークサイト上に情報が2回公開されていたことが判明している。 【東京コンピュータサービス株式会社】 https://www.to-kon.co.jp/uploads/letter.pdf https://www.to-kon.co.jp/uploads/letter2.pdf https://www.to-kon.co.jp/uploads/letter3.pdf
1月	決済サービス会社は2021年8月2日から2022年1月25日にわたり不正アクセスを受けていたことを公表した。攻撃は社内管理システムへの不正ログイン、一部アプリケーションへのSQLインジェクション、不正ファイル（バックドア）の設置など複合的なものであり、個人情報を含む情報が外部に流出していたことが判明している。 【株式会社メタップスペイメント】 https://www.metaps-payment.com/company/20220125.html https://www.metaps-payment.com/company/20220228.html
2月	一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）は、2月よりEmotetの感染が急速に拡大していることについて注意喚起した。3月にはEmotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数が2020年の感染ピーク時の約5倍以上に急増、7月中旬に観測が収束したが11月2日よりメールの配布が再度観測されるようになった。 【JPCERT/CC】 https://www.jpcert.or.jp/at/2022/at220006.html
3月	大手自動車会社は、3月1日に国内全工場（14工場28ライン）の稼働を停止すると発表した。国内仕入先におけるシステム障害とされているが、ファイルサーバにてウィルス感染を確認したと公表している。 【小島プレス工業株式会社】 https://www.kojima-tns.co.jp/wp-content/uploads/2022/03/20220331_%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E9%9A%9C%E5%AE%B3%E8%AA%BF%E6%9F%BB%E5%A0%B1%E5%91%8A%E6%9B%B8%EF%BC%88%E7%AC%AC1%E5%A0%B1%EF%BC%89.pdf https://www.kojima-tns.co.jp/wp-content/uploads/2022/08/%E3%82%A6%E3%82%A3%E3%83%AB%E3%82%B9%E6%84%9F%E6%9F%93%E8%A2%AB%E5%AE%B3%E3%81%AB%E3%82%88%E3%82%8B%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E5%81%9C%E6%AD%A2%E4%BA%8B%E6%A1%88%E7%99%BA%E7%94%9F%E3%81%AE%E3%81%8A%E7%9F%A5%E3%82%89%E3%81%9B-2.pdf
3月	自動車部品メーカ会社は、海外拠点グループ会社において3月10日にネットワークへの第三者による不正アクセスを受けたことを公表した。 【株式会社デンソー】 https://www.denso.com/jp/ja/news/newsroom/2022/20220314-01/
3月	VMware社は、Spring Frameworkに脆弱性（CVE-2022-22965）が存在し、CVE公開前にリークされたことを3月31日に公表した。脆弱性が悪用された場合、リモートから任意のコード実行が可能となる。VMware社製品以外でもSpring Frameworkを使用している他の製品に影響があり、この脆弱性は「Spring4Shell」と呼ばれている。 【VMware】 https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
4月	VMware社は、同社が提供するVMware Workspace ONE Access、VMware Identity Managerなどの製品に複数の脆弱性があることを4月6日に公表した。そのうちリモートからコード実行が可能となる脆弱性（CVE-2022-22954）とローカル権限昇格の脆弱性（CVE-2022-22960）は実際の攻撃として利用されていたことがVMware社により報告された。 【VMware】 https://www.vmware.com/security/advisories/VMSA-2022-0011.html
4月	工業部品製造会社は、グループ会社の海外工場にあるネットワークが第三者から不正アクセスを受けたことを4月8日に公表した。VPN機器の脆弱性を悪用され、侵入された可能性が高いと報告している。 【日邦産業株式会社】 https://www.nip.co.jp/news/.assets/20220408-1.pdf https://www.nip.co.jp/news/.assets/20220422-1.pdf
5月	F5 Networks社は、5月4日にiControl REST認証のバイパスが可能となるF5 BIG-IPの脆弱性（CVE-2022-1388）を公表した。この脆弱性を悪用することで認証されていない攻撃者による任意のコマンド実行やファイルの生成・削除、サービスの無効化などが可能となる。 【F5 Networks】 https://support.f5.com/csp/article/K23605346
5月	クラウド事業者は、5月7日から5月11日にかけて同社サービスで提供している一部のロードバランサに対して不正アクセスが行われていたことを公表した。 【富士通クラウドテクノロジーズ株式会社】 https://pfs.nifcloud.com/cs/catalog/cloud_news/catalog_202205161000_1.htm https://pfs.nifcloud.com/cs/catalog/cloud_news/catalog_202205311000_1.htm https://pfs.nifcloud.com/cs/catalog/cloud_news/catalog_202206071000_1.htm https://pfs.nifcloud.com/cs/catalog/cloud_news/catalog_202206291000_1.htm
5月	Microsoft社は、同社が提供するサポート診断ツールであるMicrosoft Support Diagnostic Tool（MSDT）にリモートからコード実行が可能な脆弱性（CVE-2022-30190）があることを5月30日に公表した。当該脆弱性は「Follina」と呼ばれており、ゼロデイ脆弱性であった。 【Microsoft】 https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

表-2 インシデントカレンダー(6月～12月)

月	概要・URL
6月	Atlassian社は、同社が提供するConfluence Server及びConfluence Data Centerに対して、認証不要でリモートからの任意コード実行が可能となる脆弱性(CVE-2022-26134)があることを6月2日に公表した。 【Atlassian】 https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html
6月	地方自治体は、個人情報を含むUSBメモリを6月21日に紛失したことを公表した。当該USBメモリは6月24日に発見され、11月28日に公開された調査報告書にて個人情報の漏えいは確認されなかったことを報告した。 【尼崎市】 https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html
7月	ホテルチェーン会社は、同社の委託先会社で使用しているパソコンがEmotetに感染し、11,961件の個人情報が流出したことを7月27日に公表した。 【アパホテル株式会社】 https://www.apa.co.jp/newsrelease/164149
9月	デジタル庁、総務省、文部科学省、宮内庁の4省庁23サイト及び複数の民間企業のWebサイトにおいてアクセス障害が発生した。当該事案はロシアを支持するハッカー集団「KILLNET」によるものと見られ、KILLNETは日本政府に対して宣戦布告を表明する趣旨の動画をTelegram上に投稿した。
10月	Fortinet社は、同社が提供するFortiOS、FortiProxy、FortiSwitchManagerの管理インタフェースに存在する脆弱性(CVE-2022-40684)を10月10日に公表した。当該脆弱性を悪用することで、認証をバイパスし、任意に操作できる可能性がある。 【Fortinet】 https://www.fortiguard.com/psirt/FG-IR-22-377
10月	ソフトウェア開発企業が提供するオブジェクトストレージサービスの構成ミスにより65,000を超える企業データが公開されていたことが10月19日に公表された。海外のセキュリティ企業からの通知を受け、構成の誤りを対処後、影響を受ける顧客へ通知が行われた。 【Microsoft】 https://msrc-blog.microsoft.com/2022/10/19/investigation-regarding-misconfigured-microsoft-storage-location-2/
10月	国立研究開発法人情報通信研究機構は、FocusH&S社製DVRを狙ったDDoSボット感染が増加し、6月1日から8月31日までの期間で17,489件の攻撃を観測したことを発表した。当該製品は日本国内でも販売されており利用者への速やかなファームウェアアップデートを呼びかけている。 【国立研究開発法人情報通信研究機構】 https://blog.nicter.jp/2022/10/analysis-of-ddos-bot-targeting-dvrs/
10月	医療機関は、ランサムウェアと思われる攻撃を受けたことを10月31日に公表した。攻撃により電子カルテシステムに障害が発生し通常診療ができず、一般外来も停止するなどの影響が出た。 【大阪急性期・総合医療センター】 https://www.gh.opho.jp/pdf/obstacle20221031.pdf
11月	PC周辺機器メーカは、同社が運営するWebサイトが第三者による不正アクセスを受け、ペイメントアプリケーションの改ざんが行われたことにより、最大147,545人分の個人情報と1,938件のクレジットカード情報が漏えいしたことを11月21日に公表した。 【株式会社ワコム】 https://www.wacom.com/ja-jp/about-wacom/news-and-events/2022/1484
12月	Fortinet社は、同社が提供するFortiOS SSL-VPNの脆弱性(CVE-2022-42475)を12月12日に公表した。当該脆弱性を悪用することで、認証されていない攻撃者によりリモートから任意のコードやコマンドを実行される可能性がある。 【Fortinet】 https://www.fortiguard.com/psirt/FG-IR-22-398
12月	Citrix社は、Citrix Gateway及びCitrix ADCに存在する脆弱性(CVE-2022-27518)を12月14日に公表した。当該脆弱性を悪性することで、認証されていない攻撃者によりリモートから任意のコードが実行される可能性がある。 【Citrix】 https://support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518
12月	パスワード管理ソフトウェア提供会社は、本番環境のバックアップに利用していたクラウドストレージに対して不正アクセスがあったことを12月22日に公表した。この攻撃によりサービス利用時の顧客情報と暗号化された機密情報が流出した。 【LastPass】 https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/

1.3 セキュリティトピックス

本節では、第1.2節にて取り上げた2022年のセキュリティインシデントの中から、アナリストが注目したトピックについてSOCの観測情報を紹介します。

1.3.1 2022年のEmotet

■ Emotetの概要

2022年は、2019年や2020年に多く観測され、2021年に一時収束していたEmotetの活動が再び話題となりました。Emotetは2014年に初めて報告され、当時は金融情報などを窃取するバンキングトロジャンと呼ばれるマルウェアとして知られていました。その後Emotetは機能の追加により形態を変化させ、他の端末へ感染を広げる活動を拡大しました。SOCでは2019年9月での観測を皮切りに2019年や2020年で多くのEmotetに関するメールやC&Cサーバへの通信を観測しています。2021年1月27日にEuropol（欧州刑事警察機構）によるEmotetの攻撃インフラのテイクダウンにより[*2]、2021年1月26日以降しばらくの間、Emotetの感染活動はありませんでした。しかし、2021年11月14日には別のマルウェアであるTrickbotを経由してEmotetに感染する事例が発生し[*3]、メールによるEmotetのダウンロードファイルを検出しました。2022年は、一般社団法人JPCERTコーディネーションセンター（以下、JPCERT/CC）よりEmotetの感染規模が2020年を上回ったことが報告され、前節のインシデントカレンダーの事例にもあるとおり、この活発な感染活動による被害が報告されています（表-1、表-2）。

Emotetは情報を窃取する機能や自身の拡散機能、別のマルウェアをダウンロード及び実行するローダ機能、ボットネット機能を持っています。Emotetは端末に侵入後、メールアドレス、アカウント情報、メール本文などの情報を窃取します。更に、窃取したメールの本文や件名を利用したメールを作成し、Emotetをダウンロードするファイルを添付し送信します。添付されるファイルはVBAマクロを含むMicrosoft Office形式のWord・ExcelファイルやWord・Excelファイルを圧縮したパスワード付きZIPファイルであることが知られています。パスワード付きZIPファイルはファイルの内容が暗号化されており、アンチウイルスやサンドボックスなどのセキュリティ製品で復号できない場合は検査ができません。検査できなかったファイルはセキュリティ製品の機能を回避できてしまうため、ユーザの手元に届いてしまう可能性が高くなります。2022年4月には新たな手法としてショートカットファイル（LNKファイル）やショートカットファイルを圧縮したパスワード付きZIPファイルを添付するという手法も確認されているため[*4]、従来の方法であるWord・Excelファイルだけでなく、別形式のファイルにも注意が必要です。

加えて、Emotetは前述のローダ機能を持っていることから、他のマルウェアなどの入り口としても機能しています。2022年では、Palo Alto Networks社はEmotetに感染した端末がIcedIDやBumblebeeと呼ばれるマルウェアに感染したことを確認しました[*5]。その他にも、ペネトレーションテストで使用されるCobalt Strikeと呼ばれるフレームワークをEmotetを使用して展開するという攻撃がCybereason社から報告されています[*6]。そのため、Emotetの感染をそのままにした場合、感染による被害はより深刻なものになる可能性もあります。このような特徴から、Emotetは感染力や脅威度が高いマルウェアの1つと言えます。

＊2 Europol（欧州刑事警察機構）、"World's most dangerous malware EMOTET disrupted through global action"（https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action）。
＊3 cyber.wtf、"Guess who's back"（https://cyber.wtf/2021/11/15/guess-whos-back/）。
＊4 IPA 独立行政法人 情報処理推進機構、「Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて」（https://www.ipa.go.jp/security/announce/20191202.html#L20）。
＊5 Twitter（@Unit42_Intel）（https://twitter.com/Unit42_Intel/status/1590002190298804225）。
＊6 Cybereason、「【脅威分析レポート】すべての道はCobalt Strikeに通じる – IcedID、Emotet、QBot」（https://www.cybereason.co.jp/blog/malware/7797/）。

■ Emotetの観測情報

ここでは、SOCでのEmotetの観測状況について報告します。

図-1では1年間におけるEmotetのメール件数の推移を示します。図の横軸は日付を、縦軸は対象期間における合計検出数を100%として正規化した割合を表します。

Emotetは大まかに3つの期間で検出しています。1つ目の期間は1月21日から4月5日までで、検出量が最も多い期間です。2月2日から検出が増加し、ピークは3月2日でした。これはJPCERT/CCが、Emotetに感染しメール送信に悪用される可能性のある日本のメールアドレス数が急増したことを報告している時期と一致しており（表-1、表-2）、SOCでも同様の傾向が見られました。

2つ目の期間は4月21日から7月14日までで、6月4日から観測が増加し、6月14日にピークを迎えています。添付ファイルとして、これまでのマクロ付きExcelファイルを用いたものに加え、4月30日以降からショートカットファイルやショートカットファイルを圧縮したZIPファイルも検出されるようになりました。

3つ目の期間は11月2日から11月12日までで、検出量が最も少ない期間です。この期間では、2つ目の期間に検出していたショートカットファイルは検出されず、マクロ付きExcelファイルのみを検出しています。

攻撃のメールを観測していない4月や7月から11月の時期においても、Emotet本体に変更が加えられたことが報告されており[*7]、目立った攻撃が見られない場合であっても活動は継続しているようです。

続いて、1年間におけるEmotetに感染した端末の割合を図-2に示します。図の横軸は日付を、縦軸は対象期間におけるEmotetの感染端末数の合計を100%として正規化した割合を

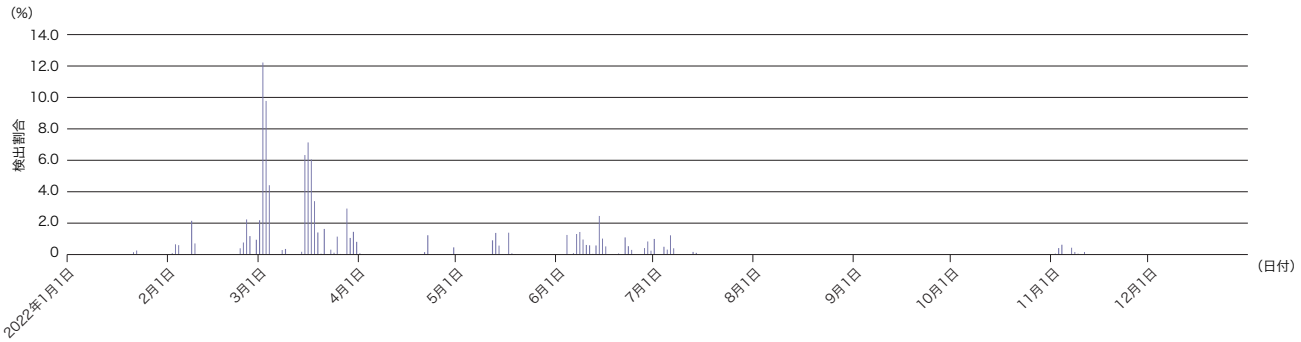


図-1 Emotetを検出したメール件数の推移

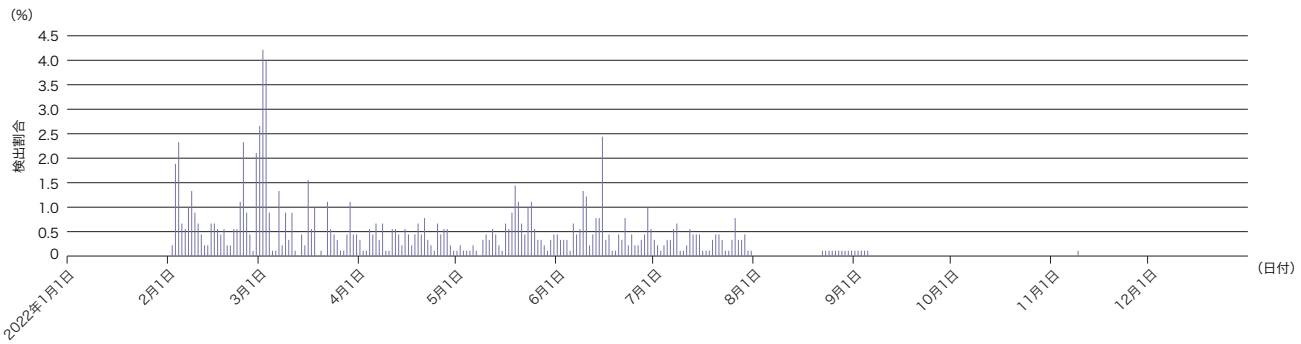


図-2 Emotetに感染した端末の割合の推移

＊7　proofpoint、「2022年秋のEmotetの復活を総合的に考える」（https://www.proofpoint.com/jp/blog/threat-insight/comprehensive-look-emotets-fall-2022-return）。

表します。なお、感染端末数はC&Cサーバへ通信を行うIPアドレスを1端末として集計しています。

感染させるメールと同様に2月2日から観測が始まり、3月2日にピークを迎えていました。4月から5月にかけては3月と比較して端末数は少ない傾向にありますが、6月15日に再び多くの端末数を確認しています。

また、端末数が比較的多い時期とEmotetを検出したメールを多く受信している時期が同じですが、Emotetを受信していない期間でも感染通信が出続けている時期があります。Emotetに感染していることにしばらく気づかなかったためと考えられ、早期発見の対策が不十分であったことが推測されます。Emotetはローダ機能を持っており、感染に気付かなかった場合は他のマルウェアに感染し被害が深刻になる可能性もあるため、早期に発見できる対策が必要です。

■ 対策

2022年12月末の時点ではEmotetの感染活動は停止していますが、再開する可能性もあり、Emotetは今後も注意するべきマルウェアの一つと言えます。EmotetはVBAマクロを含むMicrosoft Office形式のファイルやショートカットファイル（LNKファイル）を開くことで感染します。感染の被害を抑える対策として、ファイルを開いた際にマクロを実行しないようマクロの自動実行の設定を無効化することが挙げられます。Microsoft Office形式のファイルやショートカットファイルは両方ともPowerShellを実行しEmotetをダウンロードするため、業務でPowerShellを使用しない場合は、PowerShellの実行を無効にすることも対策の1つです。可能であればファイル共有の際にパスワード付きZIPファイルを用いる文化をやめ、メール受信時にパスワード付きZIPファイルを一律で遮断するような運用に変更することも有効です。

Emotetは感染拡大に用いるメールに実際に使われていたメールを使いまわしていることもあるため、人がEmotetに関するメールを見分けるのは難しい状況です。マクロの実行やショートカットファイルの開封によりEmotetに感染したことが疑われる場合は、JPCERT/CCが公開しているEmotetの感染確認ツール「EmoCheck」で確認できることがあります[*8]。また、SOCやEDRによる監視やアンチウイルスの導入といった、感染の早期発見と迅速な初動対応を行える状態にしておくことも重要です。

1.3.2 企業ネットワークへの侵入契機となるVPN機器の脆弱性

2022年は、大手企業や医療機関などの国内組織がランサムウェア感染による被害を受けた旨のニュースがたびたび報道された1年でした（表-1、表-2）。被害状況によっては事業を一時的に停止せざるを得ない状況となり、製品の納期遅れや新規患者の受入停止など、その影響は取引先や地域社会にまで拡がりました。

ランサムウェアの被害に至る主なきっかけとして「不審メールや不審サイトから受信したマルウェアへの感染」と「攻撃者による組織内ネットワークへの侵入」が挙げられます。近年、テレワークの普及によりインターネットを介して組織内ネットワークへ接続するためのVPN機器を設置する企業が増えたことから、VPN機器の脆弱性を悪用することで組織内ネットワークへ侵入される事例が目立ってきています。警察庁の調査では、2022年上半期にランサムウェア被害に遭った企業の68%が、侵入経路としてVPN機器を挙げています[*9]。

本項では、VPN機器における既知の脆弱性、及びそれらの脆弱性を狙った攻撃活動のSOCにおける観測状況を紹介します。

＊8　GitHub（@JPCERTCC）（https://github.com/JPCERTCC/EmoCheck）。
＊9　警察庁、「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について」（https://www.npa.go.jp/news/release/2022/20220914001.html）。

■ VPN機器の脆弱性

表-3は、2018～2022年の5年間にJPCERT/CCより発出された注意喚起[*10]で言及された脆弱性のうち、VPN機器に関連する14件を抽出しまとめたものです。なお、「CVE ID」は米MITRE社が管理をする共通脆弱性識別子（Common Vulnerabilities and Exposures）を、「CVSS v3ベーススコア」は米国立標準技術研究所（NIST）により評価された脆弱性の深刻度（Common Vulnerability Scoring System）を0.0～10.0の範囲で表した値をそれぞれ示しています。

■ 脆弱性を狙った攻撃活動のSOCにおける観測状況

脆弱性が残存するVPN機器を見つけたり悪用するために、インターネット上では絶えず攻撃活動が行われています。図-3は、表-3に示したVPN機器の脆弱性を狙った攻撃について、2022年にSOCで観測した検知数（割合）を示したものです。なお、図の縦軸は対象期間におけるすべての検知数を100%として正規化しています。

表-3 VPN機器に関連する主な脆弱性（2018～2022年）

公表月	製品ベンダ	CVE ID	CVSS v3ベーススコア	悪用可能タイミング	悪用による影響
2022年12月	Citrix	CVE-2022-27518	9.8	認証前	任意コード実行
2022年12月	Fortinet	CVE-2022-42475	9.8	認証前	任意コード実行
2022年10月	Fortinet	CVE-2022-40684	9.8	認証前	管理画面の認証をバイパス
2021年12月	SonicWall	CVE-2021-20038	9.8	認証前	任意コード実行
2021年9月	SonicWall	CVE-2021-20034	9.1	認証前	任意ファイルの削除
2021年4月	Pulse Secure	CVE-2021-22893	10.0	認証前	任意コード実行
2021年3月	F5 Networks	CVE-2021-22986	9.8	認証前	任意コード実行
2021年2月	SonicWall	CVE-2021-20016	9.8	認証前	認証情報やセッション情報の窃取
2020年7月	F5 Networks	CVE-2020-5902	9.8	認証前	任意コード実行
2019年12月	Citrix	CVE-2019-19781	9.8	認証前	任意コード実行
2019年7月	Palo Alto Networks	CVE-2019-1579	8.1	認証前	任意コード実行
2019年5月	Fortinet	CVE-2018-13379	9.8	認証前	任意ファイルの窃取
2019年5月	Pulse Secure	CVE-2019-11510	10.0	認証前	任意ファイルの窃取
2019年4月	Pulse Secure	CVE-2019-11539	7.2	認証前	任意のコード実行

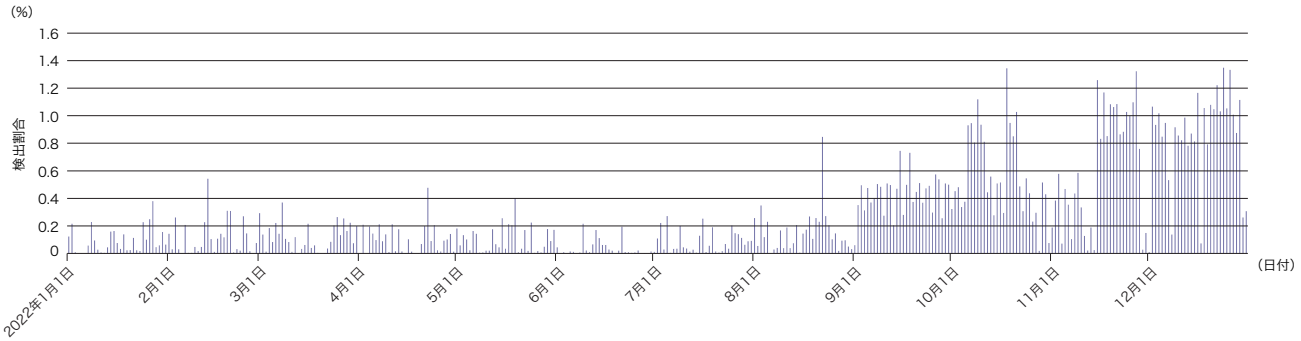


図-3 VPN機器の脆弱性を狙った攻撃の観測（2022年1月～12月）

*10 JPCERT/CC（https://www.jpcert.or.jp/at/）。

図-3より、VPN機器の脆弱性を狙った攻撃活動は年間を通じて観測され、2022年9月以降は1日あたりの検知数が増加傾向にあります。次に、2022年の1年間を通じた、表-3に示すCVE IDごとの検知数（割合）を図-4に示します。

図-4に示す脆弱性の中から、SOCのアナリストが特に注目する脆弱性を次に示します。

■ CVE-2018-13379（Fortinet社製VPN機器における任意ファイル窃取の脆弱性）

検知数が全体の91.70%を占め最も多かったのは、CVE-2018-13379でした。この脆弱性を悪用することで、攻撃者はVPN接続に必要な認証情報を窃取することができます。公表から既に3年以上が経過しているものの、今なお多くの攻撃が行われているだけでなく、実被害も発生しています。2021年10月にランサムウェア攻撃を受けた医療機関は、2022年6月に公表された報告書[*11]で、侵入の契機として当該脆弱性が悪用された可能性が高いと述べています。また、インシデントカレンダー（表-1、表-2）の10月に示すランサムウェア攻撃を受けた医療機関についても、侵入のきっかけとなった可能性が高いとされる取引業者のVPN機器で、当該脆弱性が残存するバージョンのOSが用いられていたことが示されています[*12]。

■ CVE-2022-40684（Fortinet社製VPN機器における認証バイパスの脆弱性）

CVE-2022-40684は、2022年10月に公表された比較的新しい脆弱性です。この脆弱性を悪用することで、攻撃者は認証を回避して当該VPN機器の管理画面にアクセスができることから、設定変更などにより組織内ネットワーク侵入への足掛かりとなる恐れがあります。図-4に示すとおり2022年1年間を通した検知数は1.48%であり第4位となりましたが、そのほとんどは2022年12月21日～31日のわずか11日間に検知されたものでした。2023年以降も攻撃が継続する可能性もあることから、引き続きの警戒が必要です。

■ 自組織が被害に遭わないために

自組織が同様の被害に遭わないために、ご利用のVPN機器のOSやファームウェア更新に加え、不要な機能はオフにする、管理画面など必要のない機能を外部に公開しない、接続元IPアドレスの制限を掛ける、二要素認証を設定するなどの対策を行うようにしてください。

また、現時点で組織内ネットワークへの侵入が確認できていなくとも、既に認証情報の窃取や設定変更など侵入の足掛かりを作られている可能性があることに留意が必要です。2021

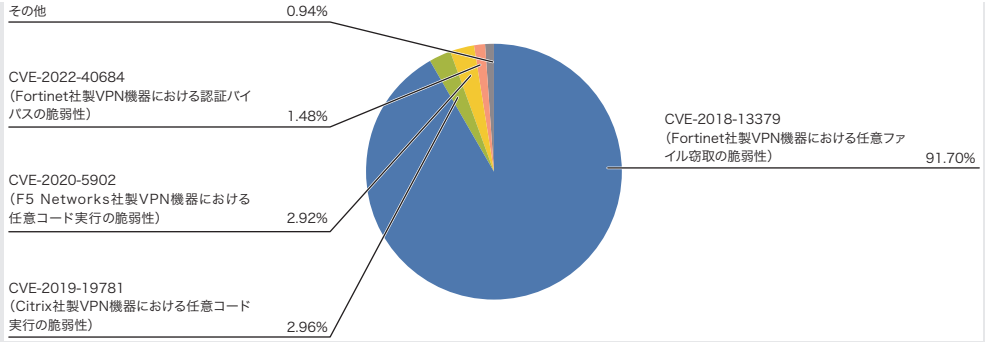


図-4 CVE IDごとの検知数（2022年1月～12月）

*11 徳島県つるぎ町立半田病院、「徳島県つるぎ町立半田病院 コンピュータウイルス感染事案 有識者会議調査報告書」（https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf）。
*12 厚生労働省、「第13回健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ資料について」（https://www.mhlw.go.jp/stf/newpage_29667.html）。

年9月、Fortinet社は全世界で約87,000台に及ぶ同社製VPN機器の認証情報が何者かによって公開されたことを発表しました[*13]。同社によると、公開された認証情報は、前述したCVE-2018-13379を狙った攻撃によって全世界のVPN機器から収集されたものであるとされています。また、公開された情報の中には、インシデントカレンダー(表-1、表-2)で取り上げたランサムウェア被害組織の認証情報が含まれていたことも判明しています[*12]。OSやファームウェアの最新化を行った際には、併せてVPN機器への不正アクセスや設定変更などの痕跡の確認、及び認証情報(パスワード)の変更まで実施するようにしてください。

1.3.3 2022年の脆弱性

表-1、表-2のインシデントカレンダーに示すとおり、2022年も複数のソフトウェア脆弱性が公表されており、それらの脆弱性を悪用した攻撃が発生しました。本項では、SOCで悪用を観測した2022年公表の脆弱性について紹介します。図-5に2022年に公表された脆弱性の悪用に対する観測割合を示します。観測数上位の脆弱性は、いずれもリモートコード実行の可能性があるものでした。リモートコード実行とは、アプリケーションに対して、特定の文字列を埋め込んだスクリプトを(HTTPリクエストによる送信などで)入力すると、入力を処理するアプリケーションサーバ上で任意のコードが実行されてしまう脆弱性です。攻撃者はこれを悪用して情報窃盗やシステムの乗っ取り、改ざん、マルウェア配布など、様々な活動を試みます。そのため、一般的にこの種類の脆弱性は深刻な脅威と判断されます。

■ F5 BIG-IP Remote Code Execution Vulnerability (CVE-2022-1388)

2022年5月4日、BIG-IPのiControlに関する脆弱性(CVE-2022-1388)が公表されました[*14]。BIG-IPはF5 Networks社製の通信制御装置であり、世界中の企業ネットワークで導入されています。iControlはBIG-IPを操作するREST API機能です。

この脆弱性では、標的のBIG-IPのiControlに対して特定の内容のHTTPリクエストを行うと、認証をすり抜け、ルート権限での任意操作が可能となります。本脆弱性を持つBIG-IPのiControlがインターネット上からアクセス可能である場合、攻

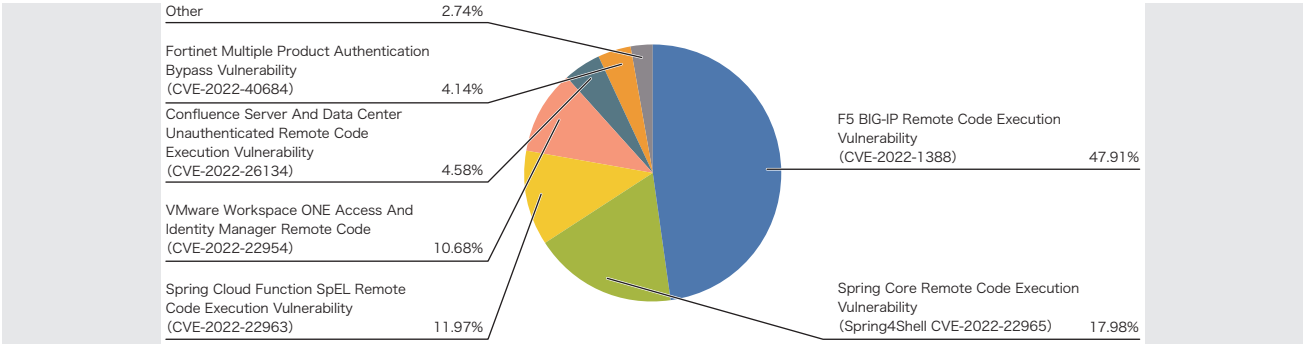


図-5 悪用を観測した2022年公表の脆弱性の割合

＊13 Fortinet、「悪意のあるアクターがFortiGate SSL-VPNの認証情報を公開」(https://www.fortinet.com/jp/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials)。
＊14 F5 Networks、"Final - K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388"(https://support.f5.com/csp/article/K23605346)。

撃者が機器の設定を任意に変更できるため、内部ネットワークへの侵入やトラフィックの盗聴などの深刻な被害に繋がる可能性があります。

図-5に示す通り、この脆弱性は2022年公開の脆弱性の中で最も多く観測しており、全体の47.91%と約半数を占めています。ソースコード管理サイトのGitHub[*15]などで本脆弱性を悪用するためのツールが数多く公開されており、それらは誰もがダウンロードして実行することができます。また、オープンソースのペネトレーションテストツールであるMetasploitにも本脆弱性を利用するコードが実装されています。Metasploitは攻撃者も悪用しており、これらのツールにより攻撃が容易に行われます。このように攻撃ツールが容易に入手できることや対象製品が世界中に普及していることから、盛んな攻撃につながっていると考えられます。図-6に、本脆弱性を狙った攻撃の1年間の推移を示します。縦軸は対象期間におけるすべての検知数を100%として正規化しています。本脆弱性は6月1日に初めて観測し、2週間後の6月18日にピークを観測しました。その後は緩やかに減少していきますが、10月中頃までは多量の攻撃を観測しました。攻撃の送信元は幅広く、6大州に渡る36カ国から送信されていました。そのため、世界中で攻撃が悪用されていることが推測できます。攻撃が減少した11月以降も断続的に少量の攻撃を観測しています。

■ Spring Core Remote Code Execution Vulnerability (Spring4Shell CVE-2022-22965)

2022年3月31日、Spring Frameworkに関する脆弱性(CVE-2022-22965)、通称「Spring4Shell」が公表されました[*16]。Spring FrameworkはJava言語のWebアプリケーション開発フレームワークであり、VMware社によりSpringプロジェクトの1つとしてオープンソースで公開されています[*17]。

本脆弱性(CVE-2022-22965)はSpring Frameworkの中核モジュールであるSpring Coreに存在する脆弱性であり、Spring Frameworkを使ったJavaアプリケーションにてリモートコード実行の危険性があります。

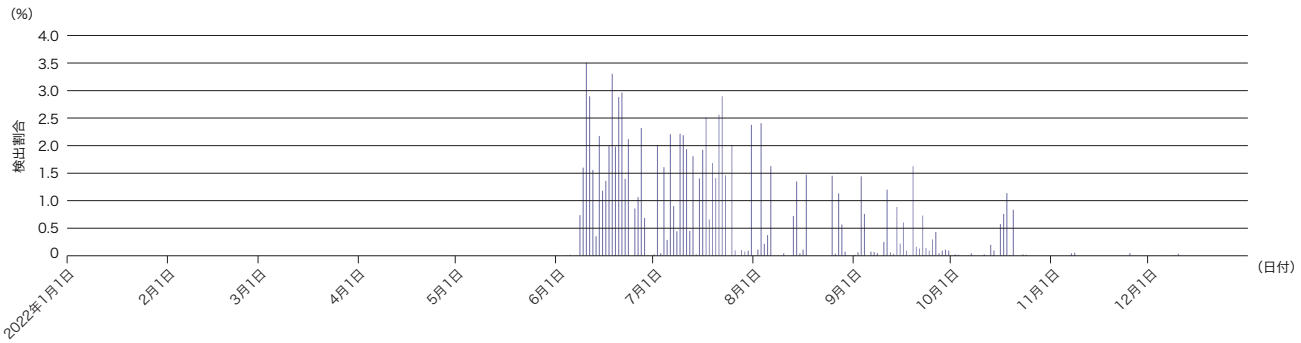


図-6 BIG-IP の脆弱性(CVE-2022-1388)を狙った攻撃の観測(2022年1月～12月)

*15 GitHub(https://github.com/)。
*16 Spring、"Spring Framework RCE, Early Announcement"(https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement)。
*17 Spring(https://spring.io/projects)。

Spring FrameworkはJava言語のWebアプリケーション開発においては、高いシェアを占めるフレームワークですが、本脆弱性の実行条件が限定的であったため、影響範囲は一部のユーザに抑えられました。

本脆弱性によりリモートコード実行が行われる場合、2段階でHTTPリクエストが送信されます。まず初めに、1回目のHTTPリクエストにてアプリケーションのロギング機能を悪用して、Webサーバ内に任意コマンドを実行するためのプログラム（WebShellと呼ばれる）が書き込まれたログファイルを作成します。そして次に2回目のHTTPリクエストにて、前段で作成したログファイル（WebShell）をURLパスに指定して任意コマンドを送信します。これにより、前段で作成したWebShellを通じて任意コードが実行されます。なお、図-7は前段のWebShellを作る通信のみで集計されています。

本脆弱性は2022年公表の脆弱性のうち、2番目に多く観測しました。

また、3番目に多く観測している脆弱性（CVE-2022-22963）もSpring Frameworkなどと同じSpringプロジェクトに関連する脆弱性です。こちらはSpring Cloudに存在した別の脆弱性です[*18]。Spring Cloudはクラウド環境開発に関するプロジェクトであり、フレームワークの根幹となるSpring Frameworkに対して使用者が限られるため、影響範囲はSpring Frameworkに関する脆弱性（CVE-2022-22965）のほうが大きいと考えられます。

■ VMware Workspace ONE Access And Identity Manager Remote Code（CVE-2022-22954）

2022年4月6日にVMware社が提供するWorkspace ONE Access（旧称Identity Manager）に関する脆弱性（CVE-2022-22954）が公表されました[*19]。

Workspace ONEはクラウド型のアプリケーションプラットフォームであり、Workspace ONE Accessはワークスペースへのアクセス管理を行うアプリケーションです。

本脆弱性は対象アプリケーションのテンプレートエンジンの処理に起因したリモートコード実行の脆弱性です。テンプレートエンジンとは、入力データをテンプレートに基づき処理してドキュメントを生成する技術です。特にWebアプリケー

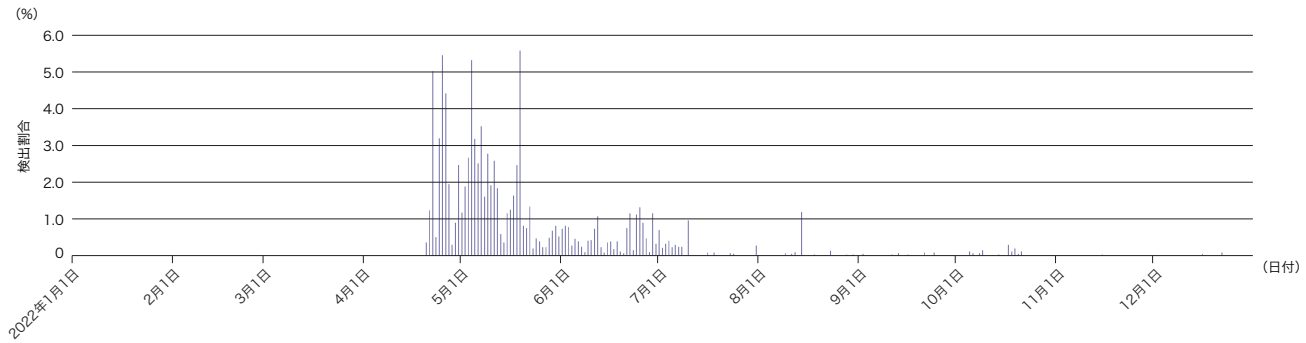


図-7 Spring Frameworkの脆弱性（CVE-2022-22965）を狙った攻撃の観測（2022年1月～12月）

＊18 VMware、"CVE-2022-22963: Remote code execution in Spring Cloud Function by malicious Spring Expression"（https://tanzu.vmware.com/security/cve-2022-22963）。
＊19 VMware、"VMSA-2022-0014"（https://www.vmware.com/security/advisories/VMSA-2022-0014.html）。

ションが動的にHTMLファイルを生成するのに使用されています。特定の文字列を含むHTTPリクエストを本脆弱性を持つアプリケーションサーバへ送信すると、その入力がテンプレートエンジンで処理され、そのサーバ上で任意のコードが実行可能となります。このような攻撃をサーバサイドテンプレートインジェクションと呼びます。

5月18日、米サイバーセキュリティインフラストラクチャセキュリティ庁(CISA)は、本脆弱性を含むVMware製品の複数の脆弱性の危険性から、米行政機関に対策を指示する緊急指令ED22-03を発行しました[*20]。2022年に発行された緊急指令はこの1件のみであり、それだけ米行政機関にとって大きな脅威となりうる危険性の高い脆弱性でした。

本脆弱性は2022年公表の脆弱性のうち、4番目に多く観測しました。また、図-8に示す通り、6月5日に初回の観測をして以降、断続的に攻撃を観測しました。8月18日は攻撃が急増しており、2番目に多く検知した10月18日と比較すると、約20倍もの攻撃数となっています。また、この8月18日の攻撃の約99.75%は単一の送信元によるものであり、一方で送信先は多岐にわたっています。この攻撃数の急増は三井物産セキュアディレクション株式会社のSOCも報告[*21]しており、単一の攻撃者が広範囲な大規模攻撃を試みた一例として見ることができます。その他、1～2ヵ月ごとに攻撃数の大きな増加が見られますが、それぞれ異なる国を送信元として観測しています。また、執筆時点(2023年1月)においても本脆弱性の悪用を継続的に観測しています。

■ Confluence Server And Data Center Unauthenticated Remote Code Execution Vulnerability(CVE-2022-26134)

2022年6月2日にConfluenceに関する脆弱性(CVE-2022-26134)が公表されました[*22]。

ConfluenceはAtlassian社が提供する企業向けWikiアプリケーションであり、多数の企業に導入されています。この脆弱性はオンプレミス版のConfluence Server及びConfluence Data Centerにおいて、リモートコード実行を引き起こす脆弱性です。サポート中の全てのバージョンが脆弱性の対象であったため、広範囲のユーザが対象となりました。また、サポートが終了したバーションを含めると2004年にリリースしたConfluence初期のバージョンである1.3.0以降の全てのバー

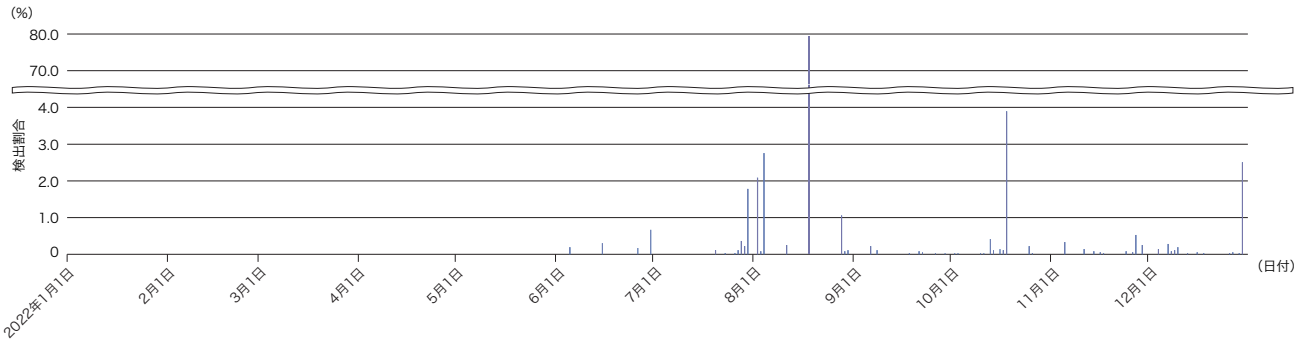


図-8 Workspace ONE AccessまたはIdentity Managerの脆弱性(CVE-2022-22954)を狙った攻撃の観測(2022年1月～12月)

*20 米サイバーセキュリティインフラストラクチャセキュリティ庁、"EMERGENCY DIRECTIVE 22-03 MITIGATE VMWARE VULNERABILITIES"(https://www.cisa.gov/emergency-directive-22-03)。
*21 三井物産セキュアディレクション株式会社、「2022年8月度 MBSD-SOCの検知傾向トピックス」(https://www.mbsd.jp/research/20220914/20228-mbsd-soc/)。
*22 Atlassian、"Confluence Security Advisory 2022-06-02"(https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html)。

ジョンに脆弱性が存在していました。なお、クラウドサービス版のConfluence Cloudはこの脆弱性の対象ではありません。脆弱性の公表時点では、修正バージョンが提供されておらず、翌日の2022年6月3日に修正されたバージョンが提供されました。

本脆弱性はOGNL（Object Graph Navigation Language）というJavaに似た式言語の実行に起因しています。HTTPリクエストの中に特殊な文字列を含めたOGNL式を埋め込み、標的のサーバに送信することで、リモートコード実行が引き起こされます。これはOGNLインジェクションと呼ばれ、この種の脆弱性は近年ではWebアプリケーションフレームワークのApache Struts2にて大きな被害を出していることで知られています。

この脆弱性は2022年公表の脆弱性のうち、5番目に多く観測しました。また、図-9に示す通り、6月18日に初めて観測し、約1ヵ月ごと間隔を開けて攻撃の一時的な増加が見られます。増加している日の多くはLinuxのidコマンドを実行しようとする攻撃コードを大量に観測しています。idコマンドが実行されても、実行ユーザの情報を出力するのみで直接的な脅威にはなりません。しかし、攻撃者が対象に脆弱性が存在するかを探索する目的で使われることが多いコマンドであり、脆弱性があることが攻撃者に知られることで、その後に危険な攻撃が行われる可能性があります。idコマンドによる攻撃コードのほかには、Linuxのwgetコマンドやcurlコマンドを利用した攻撃コードが観測されています。この攻撃コードは外部サイトから悪性のスクリプトをダウンロードし、そのスクリプトを実行します。これがサーバ上で実行されるとマルウェアがインストールされるなどの危険があります。なお、本脆弱性の悪用は執筆時点（2023年1月）においても継続して観測しています。

本項では2022年に公表された脆弱性から、SOCで多くの観測が見られた4つの脆弱性について紹介しました。対象となるバージョンは各脆弱性の参考URLから確認することができます[*14*16*19*22]。該当するアプリケーション及び対象バージョンを運用している場合は、対策済みバージョンの適用を推奨いたします。

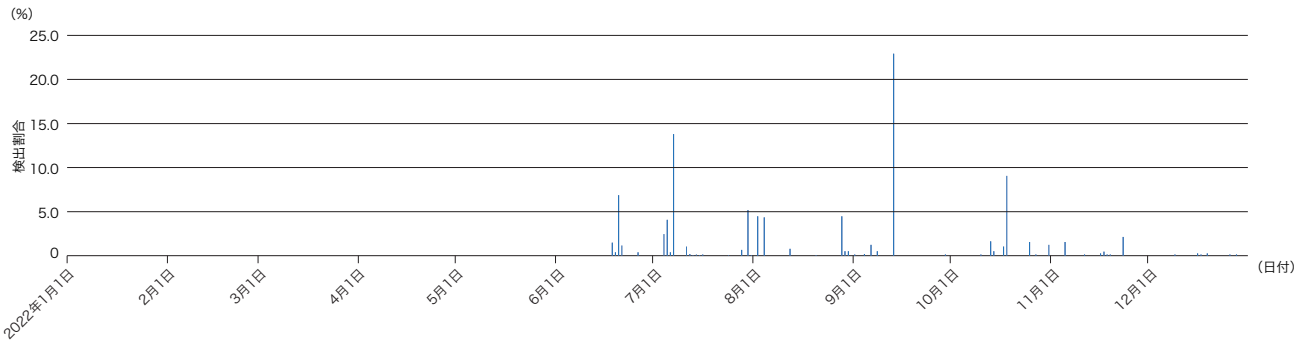


図-9 Confluenceの脆弱性（CVE-2022-26134）を狙った攻撃の観測（2022年1月～12月）

1.4 おわりに

本レポートでは、2022年に注目されたセキュリティインシデントとその中からSOCアナリストが注目したものについて観測状況を紹介しました。第1.3.1節のEmotetは2020年頃からアップデートを施しながら流行と収束を繰り返し、第1.3.2節で観測されたVPN機器を狙う攻撃では2019年に公表されたFortiOSの脆弱性（CVE-2018-13379）が最も多いなど、旧来からの攻撃であっても継続していることが分かります。大きく話題となった時だけではなく継続して警戒する必要があると言えます。一方で第1.3.3節では2022年に公表された脆弱性を用いた新しい攻撃も観測しています。利用している製品や関連サービスについて脆弱性やアップデートの情報を随時収集することも重要です。

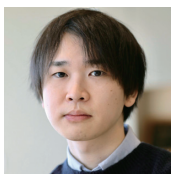
SOCでは今後もwizSafe Security Signalなどを通じて情報分析基盤で観測した脅威や、セキュリティに関するトピックなどの情報の発信をしていきますので、セキュリティ対策や業務に役立てていただければ幸いです。

執筆者：

本部 栄成（ほんぶ えいせい）
IIJ セキュリティ本部 セキュリティオペレーション部 データ分析課

宮岡 真平（みやおか しんぺい）
IIJ セキュリティ本部 セキュリティオペレーション部 データ分析課

冨山 克裕（とみやま かつひろ）
IIJ セキュリティ本部 セキュリティオペレーション部 データ分析課



西東 翔太（さいとう しょうた）
IIJ セキュリティ本部 セキュリティオペレーション部 データ分析課

データセンターと電力市場の関わり

2.1 はじめに:電力市場とデータセンター

IIJの本業である通信市場は、1985年から国内で始まった通信自由化により競争原理が導入されて以来、大きな変容を遂げてきました。電話からインターネット、固定から携帯へとサービスそのものも多様に発展し、市場規模も1985年の5兆円から、2020年には15兆円と3倍近く拡大しています。その間、料金の低廉化や、インターネット上で多様なサービスが提供されるようになり、自由化は利用者に様々なメリットをもたらしてきました。

一方、電力市場でも電力システム改革の一環で電力小売り全面自由化が2016年から始まりましたが、その進展は電気通信市場と比べ利用者への十分なメリットが現れるのに時間がかかっている状況です。電気通信市場は先行する米国というお手本があったことと、テクノロジーの進化が通信コスト(光ファイバーで送信できるデータ量が爆発的に増えた)やサービス内容(半導体の集積率が1.5年で倍増していきCPUの処理能力も爆発的に増えた)に直接的にインパクトを与えてきたのに対し、電力市場は、国家規模でモデルとなる成功事例がなく、外部からは未だ手探りで自由化が行われているように見受けられます。発電コストは化石燃料の価格や再エネ発電所の投資に依存しており、テクノロジーにより市場構造を変えるのに時間がかかるという点が、通信市場に比べ、電力市場の自由化の進展が遅い理由と考えられます。更に、ウクライナ危機を発端とした発電に必要な化石燃料コストの高騰など、世界情勢にも大きく影響を受け、電力市場の将来を見通すことは一層難しくなっています。

IIJは、電力を利用してサービスを提供し、特にデータセンターにおいてはコロケーションサービスの一部としてお客様に電力を利用していただいていることから、これまでも需要家の立場から、電力の安定供給を受けることや、コスト低減、カーボンニュートラルに向けた省電力・再エネ利用を目指して、電力事業者や機器ベンダーなどの関係者と共に取り組んできました。どの業界も電気がないと企業活動を継続できませんが、データセンターは大量に電力を消費する業種であることから、一需要家という立場を超えて、電力をめぐる様々な課題に立ち向かわなければならないと考えています。ここでは、需要家から見た電力市場の課題と、それにどのように対応していこうとしているかを説明していきます。

2.2 電力市場の課題1:電力コスト

電力市場は、「発電」「送配電」「小売」の3部門のうち、1995年の電気事業法改正により、発電部門が原則として参入が自由になりました。一方、小売部門については段階的に自由化が行われ、まず大型工場などの「特別高圧」分野、続いて中小規模工場などの「高圧」分野が自由化され、家庭向けの「低圧」分野も2016年4月に自由化されたことで、「全面自由化」が実現しました。これを機に多くの小売電気事業者が参入し、料金も低廉化され自由化の効果が表れ始めたところに、昨今の燃料費高騰による電力の調達コストの上昇により、小規模な小売事業者の経営破綻や、電力料金の値上げに至っています。

一般的にデータセンターの運営コストに占める電力料金の比率は3〜4割と言われています(図-1)。2021年3月と2023年1月との比較では燃料調整費が15.82円/kwh(東京電力 特別高圧)上昇しており、DC全体のコストが40 〜50%増えたことになります。省エネをはじめとした企業努力は継続しますが、お客様にご負担いただくことが避けられない状況になっています。

2.3 電力市場の課題2:カーボンニュートラル(省エネと再エネ)

気候変動問題に関する国際的な枠組み「パリ協定」の目標でもある「温室効果ガス(CO_2、メタン、N_2O、フロン)の排出量をゼロにするカーボンニュートラルを2050年までに達成する」ことを、世界120以上の国と地域が表明しており、日本政府も2020年10月、「2050年のカーボンニュートラル」を宣言しました。そして、政府は2022年12月「GX実現に向けた基本方針」を決定し、これにより「徹底した省エネルギーの推進」「再生可能エネルギーの主力電源化」「原子力の活用」「水素・アンモニアの導入」「電力・ガス市場の整備」「資源外交」「蓄電池産業」などの進め方や工程が明示され、今後それを実現するための法制度が整備されていくことになります。2021年10月の「第6次エネ

ルギー基本計画」でも、図-2のとおり2030年のエネルギーミックスで9%程度の省エネと、従来22～24%だった再生可能エネルギー比率を36%～38%程度に増やすことが数値目標として示されています。IIJも需要家として、カーボンニュートラル実現に向けた省エネ・再エネを、主体的に取り組むべき課題と捉えています。

■ カーボンニュートラルデータセンターモデル

カーボンニュートラルの実現には、電力を供給する発電設備とそれを消費するDCが有機的に結合した新しいモデルの創出が求められます。IIJでは、省エネ技術をベースに、複数の発電所群、蓄電設備、需給制御などを組み合わせた「カーボンニュートラルデータセンターリファレンスモデル」(図-3)を考案し、ビジネス・技術の両面から技術実証や社外パートナーとの協力を進めながら、自社DCの改修・新築に適用していきます。

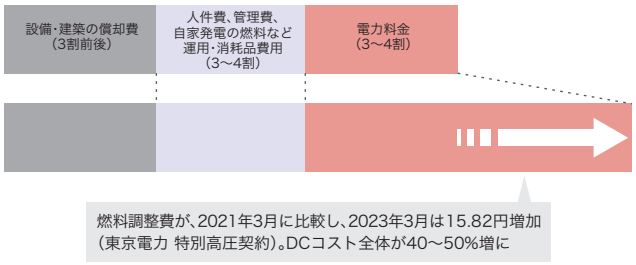


図-1 一般的なデータセンターのコスト構造*1

■ 省エネの動向とIIJの実績

2022年に省エネ法が改正され、データセンター業にベンチマーク制度が導入されました。PUE(Power Usage Effectiveness)がベンチマーク指標に採用され、1.4以下を目指すべき水準と

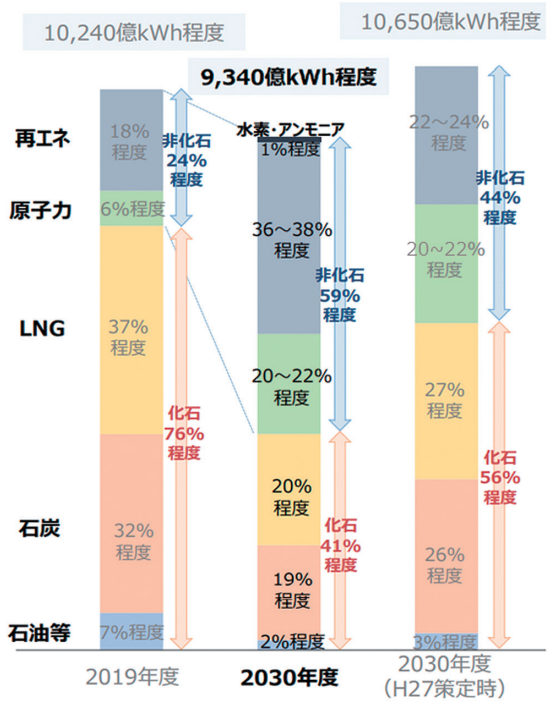


図-2「第6次エネルギー基本計画」のエネルギーミックス*2

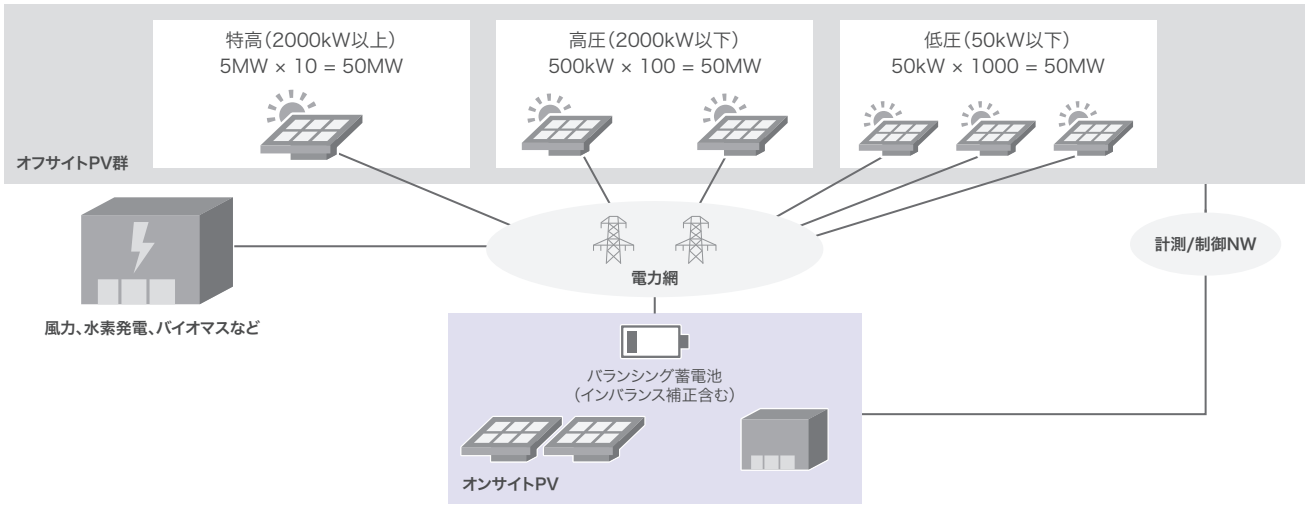


図-3 カーボンニュートラルデータセンターリファレンスモデル

*1　出典：日経クロステックHPからIIJが一部修正(https://xtech.nikkei.com/atcl/nxt/column/18/02096/063000007/)。
*2　出典：資源エネルギー庁HP(https://www.enecho.meti.go.jp/about/special/johoteikyo/energykihonkeikaku_2022.html.html)。

定められました。データセンター業を営む企業は2023年7月に1回目の報告を行うことになりますが、電力を効率的に利用する省電力化をより一層進めることが法的に定められたことになります。

PUEは「データセンター施設全体のエネルギー使用量」を「IT機器のエネルギー使用量」で割った値で、1に近いほど高効率とされ、日本では1.7程度が平均値と言われています。全世界のデータセンターを対象としたUptime Instituteの調査では、2022年は1.55と2007年の2.5から大幅に改善されています。

全世界のデータセンターが消費する電力は2030年までに世界の電力の51％に達すると言われ、データセンターの消費電力の増加は環境に深刻な影響を与える問題と捉えられていました。しかし、2020年にアメリカのローレンス・バークレー国立研究所などの共同調査により、2010年から2018年にかけて、データセンターの処理容量が6倍増えているのに対し、消費電力の伸びは2010年全世界全体の1％に相当する約194TWから、2018年には約205TWと6%増えただけであると報告されました。

図-4は、データセンターを、Traditional(従来型コロケーション)、Cloud(non-Hyperscale)、Hyperscale(クラウド事業者向け

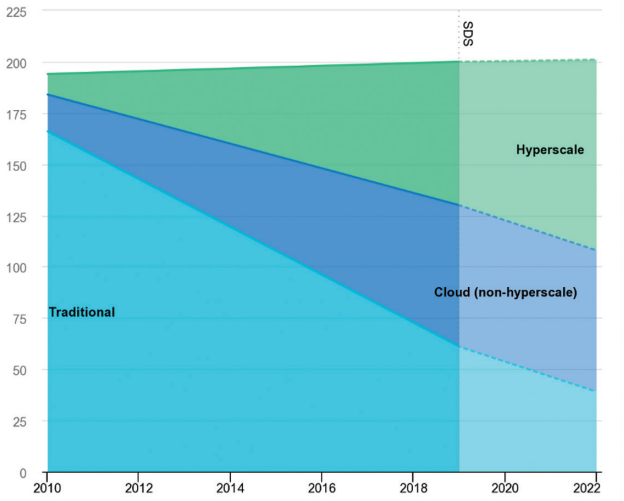


図-4 全世界のデータセンターの電力消費量*3

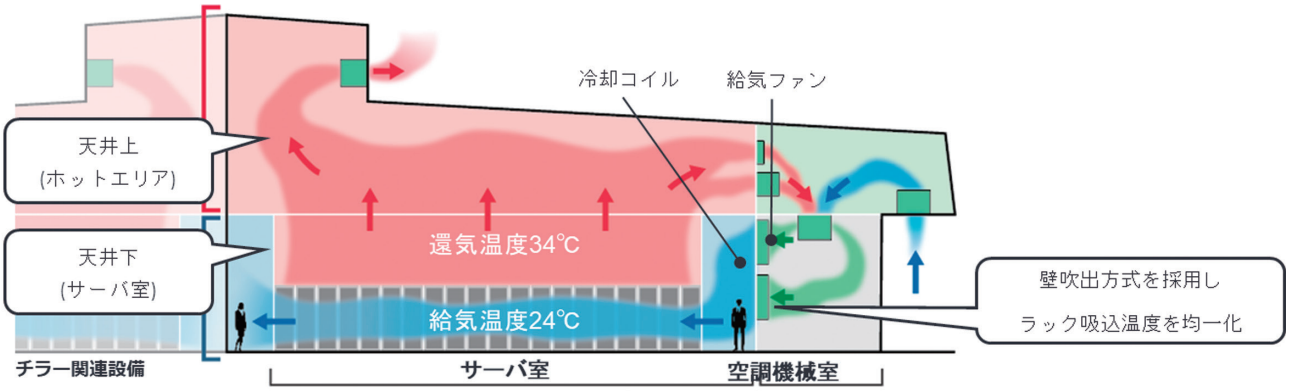


図-5 白井データセンターキャンパスの外気冷却方式空調

*3　出典：IEA（https://www.iea.org/data-and-statistics/charts/global-data-centre-energy-demand-bydata-centre-type-2010-2022）。

大規模DC)の3種類に分けてそれぞの消費電力の推移を示したものです。Hyperscaleの比率は2010年と比べ、2018年には3割近く伸びており、少ない消費電力で多くの処理が可能なHyperscale DCの普及により、データセンター全体の消費電力増大が抑えられ、PUEの改善につながったことが要因の1つと考えられます。

■ IIJ の取り組み

IIJは島根県松江市と千葉県白井市の2ヵ所に自社データセンターを運営しており、そこでは省エネ技術を導入し効率的な運用を実現しています。データセンターでIT機器に次いで多くの電力を消費する空調設備に外気冷却方式を採用し(図-5)、またIT機器に給電する電圧を230Vに統一することにより、UPS (停電対策用蓄電池)の400V出力電圧を損失のない無変換でサーバに給電できる3相4線式を採用すること(図-6)などにより、PUE1.2を実現しています。

図-7、図-8はPUEの実績値です。松江データセンターパーク(以下、松江DCP) は2011年に開設し、2017年から安定的にPUE1.2台を達成しています。白井データセンターキャンパス(以下、白井DCC)は、2019年に運用を開始し、稼働率が上がるに従いPUEは改善され、2022年度は1.3台を達成する見込みです。

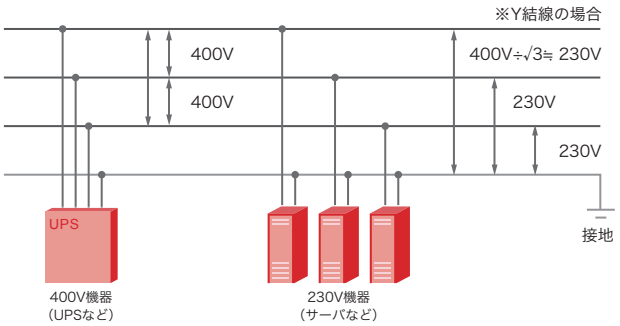


図-6 3相4線方式原理

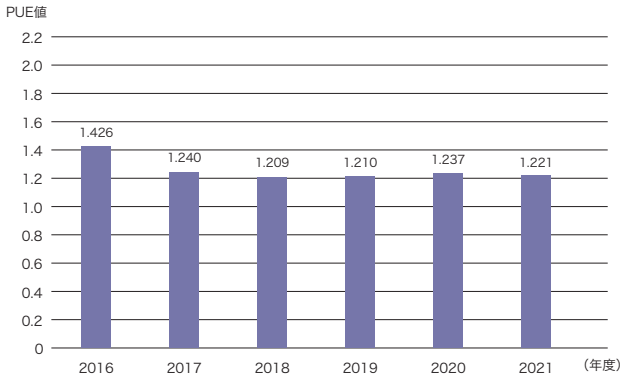


図-7 松江データセンターパークのPUE(年間平均値)の推移

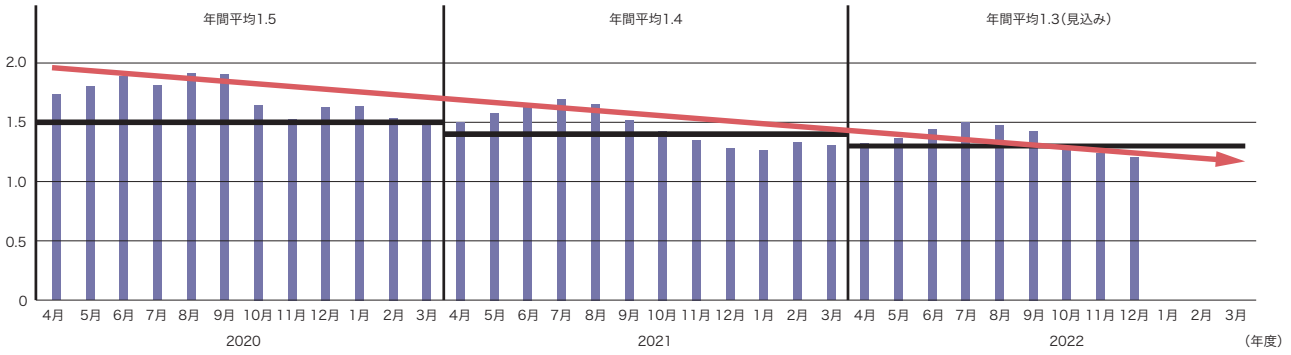


図-8 白井データセンターキャンパスのPUE(月平均値)の推移

■ 再エネの動向と取り組み

ハリウッドで映画化が進むSF小説の『プロジェクト・ヘイル・メアリー』には、太陽光エネルギーを大量に集めるためにサハラ砂漠の4分の1にパネルを敷き詰めた結果、スペインで竜巻が多発するなど、誘発された自然災害により人類が甚大な被害を被る場面がありますが、小説の中だけでなく、太陽光パネル設置のために環境が破壊され地すべりなどの被害が現実に発生し、廃棄後のパネルの処理問題が顕在化するなど、国内においては普及に向けてクリアする課題が多くある状況です。

しかし、図-9のとおり2022年12月EIAは、2027年までの今後5年間に、世界の再エネ発電容量は、現在の中国の全発電量に相当する2400GW(2.4TW)増加すると報告しており、再エネの普及は世界的に加速していくと考えられます。

特にIT業界はグローバルでは最も再エネ導入が進んでいる業界です。図-10は、再生可能エネルギーを発電事業者から直接購入するPPA(Power Purchase Agreement)に基づく電力調達量のトップ10を示していますが、10社のうち5社(Google、Facebook、Amazon、Microsoft、QTS)がデータセンターオペレーターです。再エネの利用は、IR的な効果はもちろんありますが、グローバルでは風力や太陽光による再エネの発電コストが従来型の化石燃料による発電コストよりさがっているため、大量の電力を定常的に消費し続けるデータセンターオペレーターにとっては、再エネへのシフトも経済合理性のもとに進められているのです。

IIJでも「再エネ化」の取り組みを進めており、松江DCPでは電力会社の電力にエネルギー属性証書を付加する実質再生可能エネルギー由来の電力を2022年2月より導入しました。事業活動で消費するエネルギーを100%再生可能エネルギーで調達することを目標とする国際的イニシアチブの「RE100」で、加盟企業に求める技術要件が2022年10月に改訂され、小売事業者からの電力購入やエネルギー属性証書においては、発運転開始・設備増強から15年以内の電源からの再エネ電力のみRE100適合になり、今後は自家消費のためにオンサイトの発電設備を新設することやオフサイトのコーポレートPPAの導入が加速していくと考えられます。更に、2023年4月に改正

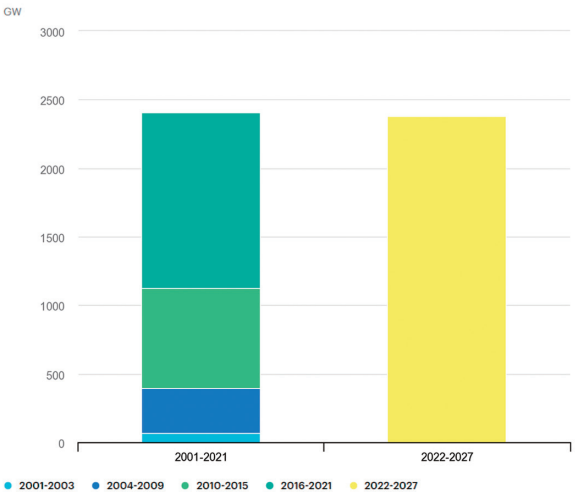


図-9 2021-2027の再エネ電力増加量*4

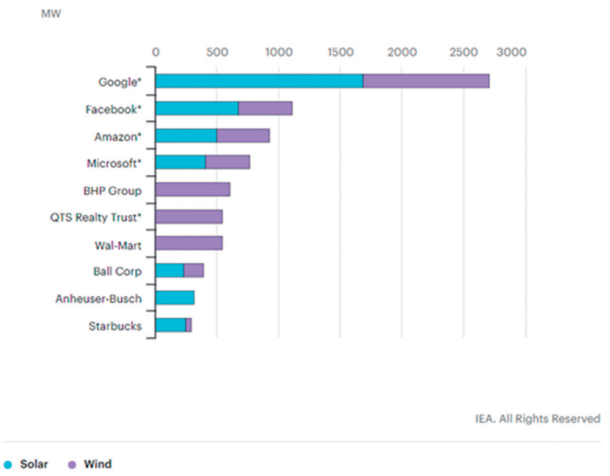


図-10 PPA 契約量 トップ10(2019)*5

*4　出典:IEA Renewables 2022(https://www.iea.org/reports/renewables-2022/executive-summary)。
*5　出典:IEA(https://www.iea.org/commentaries/data-centres-and-energy-from-global-headlines-to-local-headaches)。

予定の省エネ法では、非化石エネルギーへの転換に関する措置が新設され、非化石エネルギーの使用状況の報告が求められるようになるため、再エネ導入に取り組む企業がより一層増えることが予想されます。

図-11のように、松江DCP・白井DCCともにオンサイト型の太陽光発電設備を2022年度中に稼働させる予定ですが、オンサイト型の発電設備から得られる電力はDC 全体に対し小さい(数%程度)といった課題があります。再生可能エネルギーの発電コストは年々下がっていることもあり、オフサイト型のコーポレートPPAや、発電所を保有する自己託送を次のステップとして検討していきます。

2.4 電力市場の課題３：新市場創設による電力安定供給

■ 新たな市場への参入 容量市場

東日本大震災を転機に、「電力安定供給確保」「電気料金抑制」「需要家の選択肢／事業者の事業機会拡大」を目的として、2015年から段階的に電力システム改革が進められ、図-12に示す新たな取引市場が創設されました。

新市場の1つである容量市場は、「電力市場自由化」及び「再エネ電力導入拡大に伴い再エネ以外の電源の稼働率低下や市場価格の低下」などにより、投資回収の予見性が低下し新しい発電設備への投資が進まないリスクを低減し、将来にわたる電力の

図-11 オンサイト太陽光発電設備の導入

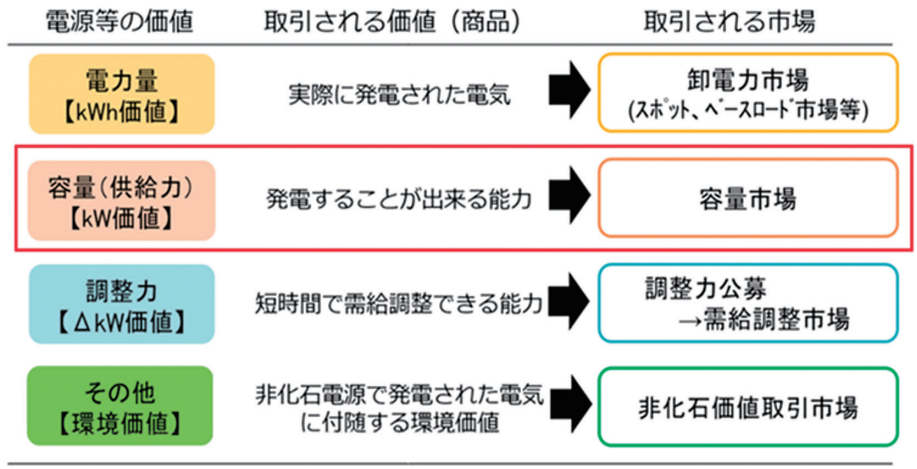


図-12 新たな取引市場*6

*6　出典：電力広域的運営推進機関HP(https://www.occto.or.jp/capacity-market/shikumi/capacity-market.html)。

供給力を確保するために、電力量(KWh)ではなく将来の供給力(KW)を取引する市場です。

この容量市場で取引される「安定電源」、「変動電源」、「発動指令電源」のうち、発動指令電源として、関西電力がアグリゲートする「バーチャルパワープラント(VPP)[*7]」の一部として、IIJは2024年度から電力の供給を行います。白井DCCで、夏場の空調用電力の平準化のために導入しているBCP用のリチウムイオン型蓄電池を活用し、VPPの電力需給コントロールの1つに位置付けられるデマンドレスポンス(DR)[*8]において、蓄電池の余力やオンサイト太陽光発電を活用して電力使用の抑制要請に応じ、アグリゲーターから報酬を得ることで、データセンターの運用コストの低減を図ります(図-13)。

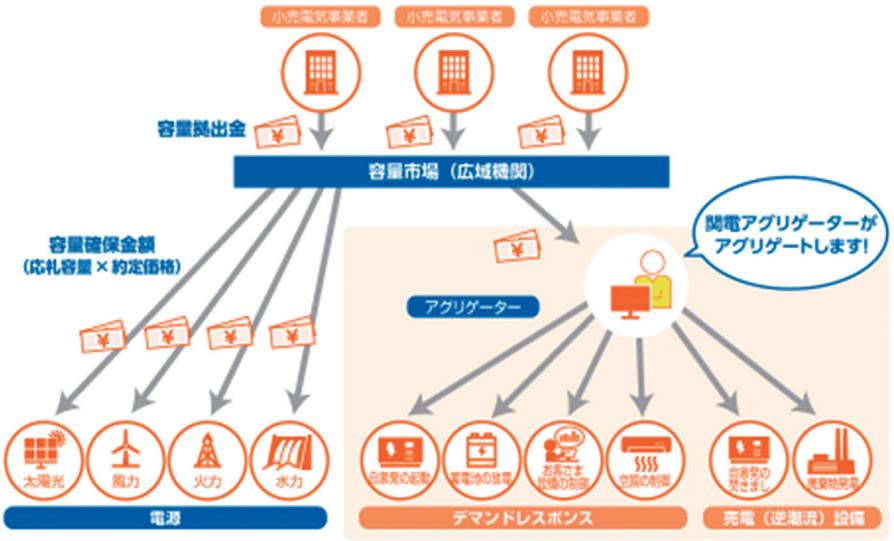


図-13 容量市場参画のイメージ[*9]

*7 VPP(Virtual Power Plant=仮想発電所):企業や自治体が所有する蓄電池や小規模発電施設など、地域に分散した電源設備を、アグリゲーターと呼ばれる事業者が統合的に制御することで、あたかも1つの発電所のように機能する仕組み。

*8 DR(Demand Response):電気の需給バランスをコントロールするために、「時間帯別に電気料金設定を行う」、「ピーク時に使用を控えた需要家に対価を支払う」などの方法で需要家側の電力使用量を制御すること。

*9 出典:関西電力HP(https://www.kepco.co.jp/energy_supply/energy/vpp/market.html)。

2.5 最後に

データセンターという需要家として、電力市場の課題にどのように対応しているか述べてきましたが、最後にIIJが、データセンターの利用者に対して、電力供給の面で提供していきたいことを説明します。

まず1つは、電力の見える化です。今後は、データセンターの利用者にも、これまで以上に省エネが求められていくと考えられます。そのため利用者もどのくらい電力を利用しているか知る必要があります。顧客ごとに電力消費の現状を把握できるような情報をきめ細かく提供できる仕組みを、なるべく早く整備していく計画です。

もう1つは再エネ価値の提供です。カーボンニュートラルの取り組みは広がっていくことになりますが、データセンターで利用者が使う電力の再エネの比率や種別を見える化することをベースに、再エネの環境価値そのものを顧客に提供できるようなプラットフォームを構築していくことも検討しています。

大量の電力を消費するデータセンターを運用する企業としての社会的な責務として、カーボンニュートラルの実現に向け、より一層のチャレンジを継続し成果を報告できるよう、取り組んでいきます。

執筆者:
久保 力（くぼ いさお）
IIJ 基盤エンジニアリング本部 基盤サービス部長。
2008年にIIJに入社。データセンター事業を統括し、松江DCP、白井DCCを構築。早期のカーボンニュートラル実現を目指す。

新設「IIJ Studio TOKYO」将来への架け橋

3.1 はじめに

ISPの会社として認知されているIIJですが、実は1990年代から映像配信事業を行っています。ここ数年は「IIJ MediaSphereサービス」をはじめ、大規模コンテンツ配信サービスなどの提供を積極的に行い、より多様化するお客様のニーズに応えられるよう、サービスの拡充を進めてきました。そして社会情勢が大きく変化した2020年以降、オンラインの配信が増え、それに伴い多くの企業が動画配信を行うようになってきています。IIJも自社の決算発表会など社外に向けた配信を行い、企業のブランディングにもつながる映像・音声の品質に対して高い評価と、同じように配信を実施したいという声も頂きました。決算発表の配信では、会議室に仮設したカメラやスイッチャー(映像信号を切り替える装置)を用いて広報部や複数部署のメンバーで運営するという、現場のスタッフの知識と経験をフルに活用し、安定した高品質の配信を実施していました。ただ、配信場所が普通の会議室だったこともあり、外から入る雑音や突発的なアクシデントなどに悩まされることが度々あったのです。更に、IIJは毎年春に日本最大級のクラシック音楽の祭典「東京・春・音楽祭(以降、春祭)」の配信を行っており、2021年の開催から有料ライブストリーミング配信を行っています。2021年は上野文化会館内に仮説の配信センターを構築し、複数の会場からの映像を文化会館で受けとり、そこから配信する形をとっていたため機材の運搬や配信センターの構築など、配信以外のところでかなりの負荷がかかっていました。そのため、翌年の2022年は、配信センターをIIJ飯田橋オフィス内に構築し、上野文化会館のホールに設置したIPリモートカメラを飯田橋からコントロールし、現地からの映像を飯田橋のサブコントロールルームへ送り配信する「リモートプロダクション配信」を実現しました。

ただ、2021年及び2022年ともにその都度配信センターを構築する作業が必要で、場所の確保や機材の調達など様々な課題もありました。こうした社内外からの映像配信の需要・ニーズの高まりを受け、更に、より多くのお客様からの要望にも応えられるよう、常設の配信センターを構築し、高品質で安定した配信に対応できる常設スタジオの検討を開始したのです。

そして2022年10月、ついに「IIJ Studio TOKYO」が飯田橋に誕生しました。ただし常設のスタジオができただけでは高品質の配信を行うことはできません。安定した映像制作・配信環境を構築するには長時間のエージングや検証、オペレーターの熟練度や経験、そしてチームワークも含め運用に向けて非常に多くの作業と時間を要します。

更に社内には映像制作に関する知識を有する者も多くなく、オペレーターの育成や機材の扱い方、ケーブルの巻き方、求められる映像・音声の品質のレベルなども含め一からのスタートになりました。

2022年度は主に社内の配信や映像収録を中心に設備・機器の知識や使い方、運用体制の構築など手探り状態で進めてきました。ただ、社内で完結していては独りよがりになってしまいます。来年度以降のサービス化を想定し、よりよいスタジオ運用を目指すため、スタジオ作りと同時に社外とのコミュニケーションを積極的に行ったり、内部からのフィードバックや意見を集めるなど、社内外のコミュニケーションの活性化と外部パートナーとの連携強化を進めています。

また、本章で紹介する映像業界の課題にも挑戦すべきと考えました。IIJらしさ、IIJが作るスタジオとはどのようなものかという点から、IT・IPをベースとしたリモートプロダクションにも対応でき、モバイル回線を利用した中継映像の利用なども可能なスタジオの計画を行いました。

本稿では、現在の映像制作にIPを用いることで得られるメリットや課題、そして「IIJ Studio Tokyo」の設備について紹介します。

3.2 IIJ Studio TOKYO 設備の概要

ここではIIJ Studio TOKYOの設備について説明します。

IIJ Studio TOKYOには図-1のとおりスタジオ(写真-1)と6つの部屋があり、部屋同士が10Gbpsまたは1GbpsのネットワークでIP接続されています。スタジオシステムをIPで構成するメリットは、光ファイバーケーブル1本でスタジオサブ(写真-2)と接続可能な点です。例えば別フロアの大会議室などにカメラを設置することで、会議室を簡単に仮設スタジオに変えることができます。また、撮影の規模や観客の有無など目的に応じて柔軟な撮影、会場の構築ができるようになります。更に、リモートプロダクションの要素を持ち合わせることで、準備に多くの

写真-1：スタジオ

写真-2：スタジオサブ

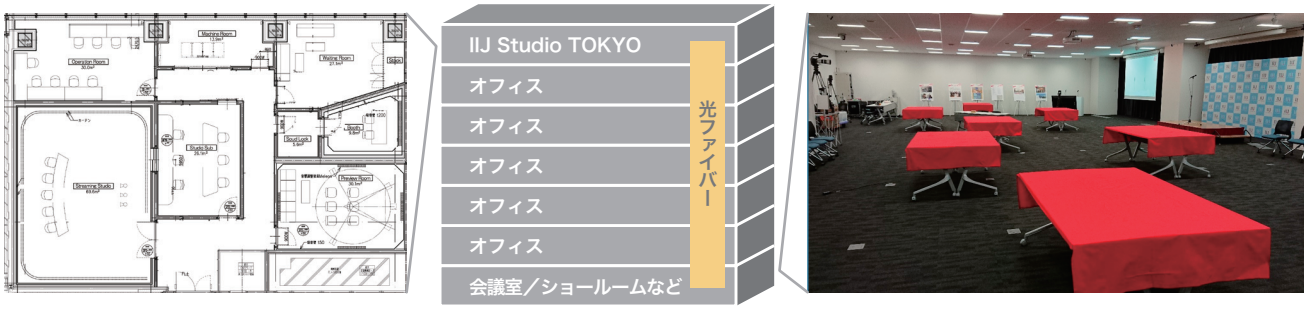


図-1 スタジオ配置図とネットワーク構成

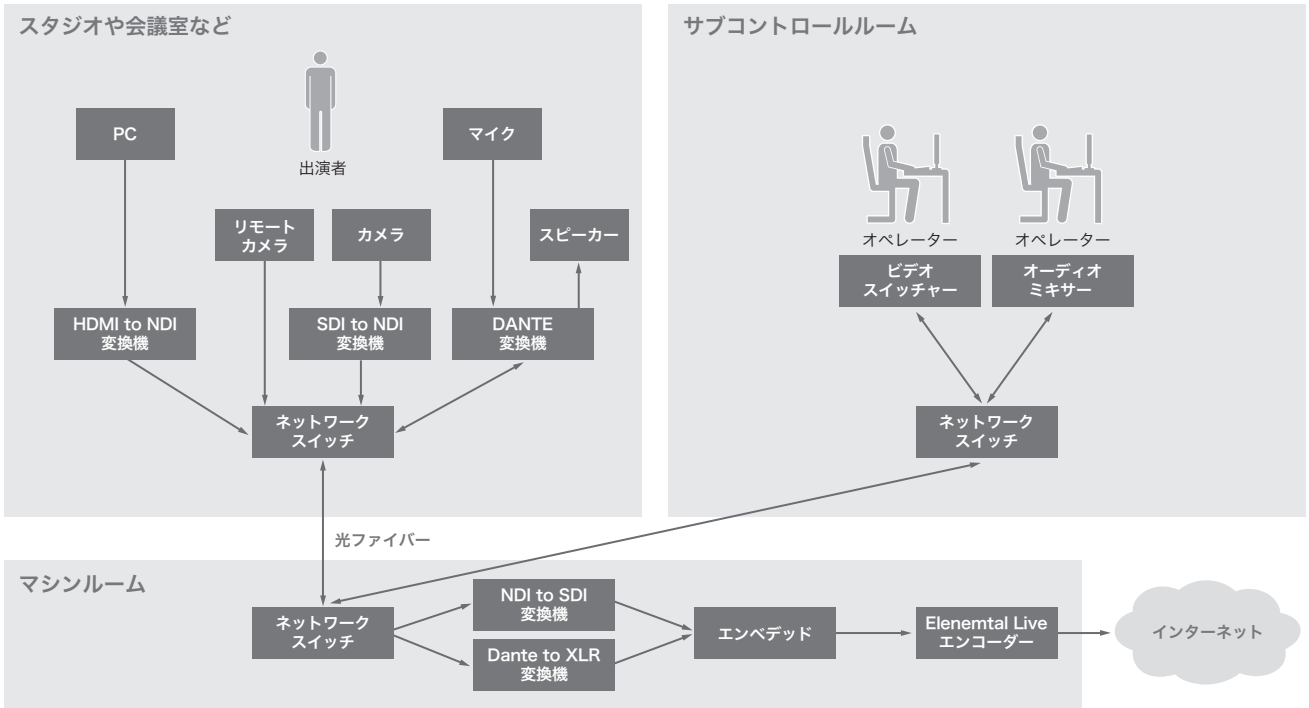


図-2 構成例
※IP利用のみを想定した図です。SDIも併用してオペレーションすることも可能です。

時間を要する複数カメラの画角や色味の調整をスタジオサブ内で一元的に管理でき、現地のカメラマンやオペレータの削減や作業負担の軽減などにもつながります。

■ スタジオ

■ カメラ

スタジオには撮影に使用するカメラが全部で6台（SONY社のプロフェッショナルカムコーダー2台とPanasonic社のリモートカメラ4台）あり、様々な画角で映像制作できます。基本コンセプトとしてリモートカメラをメインにすることでカメラオペレーターの人員不足にも対応します。そしてそれらのカメラで撮影するスタジオでは、利用者の要望に合わせて様々なシチュエーションに対応できるよう白壁や黒カーテン、クロマキー合成できるようグリーンカーテン・グリーンマットを用意しています。また、撮影に欠かせない照明はBluetooth接続でiPadから光量や色温度のコントロールが可能です。

■ マイク

ワイヤレスマイクは安定性の観点から混線防止対策として、免許が必要なA型ラジオマイクを利用しています。ピンマイクとハンドマイクで、目的に合わせて使い分けられるようにしています。また、万が一のトラブルに対応するために無指向性コンデンサーマイクを天井に設置し、スタジオ内の音声を確実に収録可能にしています。

■ スタジオサブ

■ スイッチャー

スタジオサブでは、IPスイッチャーとしてNewTek社のTriCaster 2 Eliteを採用しています。SDIも8系統、更にNDIを32系統入力できます。そのため配線の省略化により、映像ソースを送出する機材の設置場所や数の自由度を高めることができます。

また、ソフトウェアスイッチャーならではの機能「バーチャルセット」を用いることで、1台のカメラで空間に動きのある表現が可能となり、映像制作の幅が広がります。他に、サブスイッチャーとしてPanasonic社のスイッチャーも設置しているため、スタジオでの撮影をメインスイッチャーで実施しながら、サブスイッチャーでリモートプロダクションを同時に行なうといった複数のオペレーションができます。

■ デジタルミキサー

スタジオで扱うオーディオプロトコルには「Dante」を採用しました。Dante機器で構成することでDante Controllerやデジタルオーディオミキサーでのルーティング設定をPCアプリ上から簡単な操作で切り替えることができ、物理配線を変えることなく必要な音源を必要な場所に素早く送出できます。

■ マシンルーム

すべての映像信号をマシンルームに集約することで、無駄な配線を減らしました。必要な部屋や機材に適切な映像のルーティングを効率的に行えます。また、外現場からの中継も容易に実施できるよう、小型の映像中継機「LiveU」の受信機を常設しており、春祭などでの利用を想定しています。また、インターネット配信用の「Elemental Live（エンコーダー）」も常設し、スタジオからの配信、外部からの映像入力などに利用できるようになっています。更に、インターネット回線は10Gbpsの専用線を引き込み、IIJバックボーンと直結することでIIJの強みを活かした通信環境を提供しています。

■ 録音ブース

IIJ Studio TOKYOには音声収録専用の部屋があります。スタジオでの収録に合わせてナレーションを入れたり、ウェビナーなどの司会の音声を事前に収録することが可能です。音声収録に最適な環境を提供するため、床や壁の音の反響を抑えるよう考慮した作りになっています。既存の空調設備を専用ダクトに取り換えたり、入った瞬間に耳に入る音の質が変わるのが分かるほど部屋の形や吸音材の設置位置にも配慮しました。

■ 試写室

100インチの大型スクリーンで7.1.4chのDolby Atmos対応の音響設備で作品を試写できます。また、出演者の控室や対談などの撮影場所としても利用できます。

■ 控室

神楽坂方面を見渡せる眺望で出演時間までリラックスできます。また、化粧台や着替え用のカーテン、大きな収納スペース、冷蔵も完備しています。こちらもインタビューや対談、ディスカッションなどの撮影も可能です。動画だけではなく、スチルの撮影にも使えます。

■ 運用室

運用室はスタジオで使う機材の保管や検証、撮影・収録した映像の編集など、スタジオ運用の作業場所として用意しています。春祭などの大規模配信では複数同時に配信・監視対応しなければならず、サブに２系統、運用室に２系統設置し、最大4つの配信を同時に行うことができるように機材を用意しています。その為の大きなモニターを設置して配信ステータスを確認できる部屋となっています。

写真-3：録音ブース

写真-5：控室

写真-4：試写室

写真-6：運用室

3.3 なぜIPなのか？映像業界の課題とIPのメリット

映像業界では、かねてよりベースバンド信号（コンポジット信号やSDI信号など）を利用した映像制作が主流で、50年以上も変わらずこのベースバンドスイッチャー（電子回路設計）を利用した「Live映像制作」が行われています。かつてアナログ回路のスイッチャーが使われていた頃は、電源投入後、数時間経たないと信号が安定しない・映像レベルが変わってしまうなどの特徴があり、扱うには熟練の経験と技が必要でした。それから数十年を経て登場したデジタルスイッチャーでは電源投入後から安定したオペレーションが可能になりましたが、ここに来て、8kなど更なる映像の高画質化への対応で、スイッチャーに接続する12G同軸ケーブル（SDIケーブル）の伝送帯域やケーブル長に限界点が見え始めています。

一方、IPの世界では10G、25G、100Gと通信帯域が格段に向上し、進化のスピードに差が出てきているのが現状です。このように「Live映像制作」は数十年を経て変革の時代を迎えています。

旧来のSDIはIn・Outどちらか片方向のみの伝送しかできませんが、IP映像伝送は1本のケーブルで複数の映像を送受信することが可能です。また、圧縮技術を用いて容易に映像の送受信が行え、限りあるリソースの中で柔軟に設計することができます。これは、大規模になればなるほどルーティングスイッチャー（映像を各機器へ相互的に分配する装置）やケーブルの配線本数などシステム構築に大きな影響を与えます。

圧縮映像は、既に「ポストプロダクション映像制作」領域で利用されています。2000年頃以降にリニア編集（ベースバンド編集）からAvid / MediacomposerやApple / Final Cut ProなどPCベースでのノンリニア編集（ファイルベース編集）へ変革し、現在ではノンリニア編集が定着化しています。しかし、「Live映像制作」の分野では信頼性やノウハウが蓄積されておらず、圧縮映像やIP映像をメインに「Live映像制作」が行われていないのが現状です。「Live映像制作」がIPやPCベースで行われない要因としては、以下のような項目が課題としてあります。

写真-7：同軸ケーブル

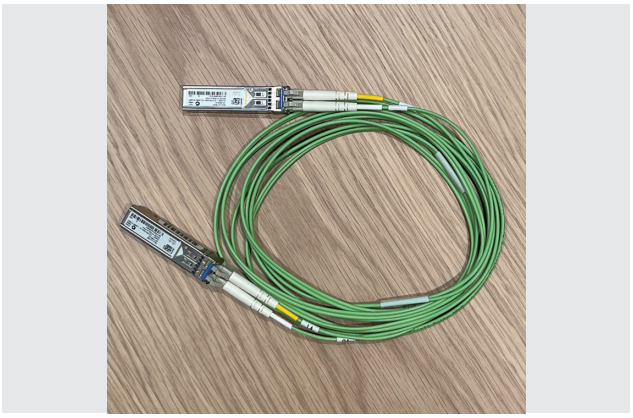


写真-8：光ケーブル

- **NDIを含むIPスタジオのデメリットや課題**
  - IT技術者の不足
  - SDIとは異なり接続しただけでは信号のやり取りができない・設定が必要
  - 安定性への不安や監視の複雑さなど未経験の部分がある
  - 慣れ親しんだ作法やケーブリング・周辺機器などラインナップが未成熟である
  - 情報不足

IIJでは、映像が得意な人員とIPが得意な人員が協力することで上記のような課題に取り組み、安定して使いやすい環境の提供を目指しています。

「Live映像制作」で採用する代表的なプロトコルはいくつかあります。今回のスタジオには圧縮技術とIP技術の良いところを掛け合わせたNDI (Network Device Interface)を採用しました。次項ではNDIの特徴やメリットについて述べます。

3.4 NDI(Network Device Interface)のメリット

NDIは8bitから12bitまでサポートされています。アルファチャンネル(RGB以外の透明度)の採用などにより合成作業に対しても柔軟で、ノンリニア編集機とも親和性が高く、ポストプロダクションワークフローへスムーズかつ容易に引き継ぐことができます。リモートプロダクションへの発展などを見据えて、現時点ではNDIが将来性、汎用性、コストパフォーマンスに優れていると考えました。また、NDIは様々なデバイスやOSとのシームレスな連携を得意としており、Teamsアプリやスマートフォンでも扱える汎用性の高さを持っています。放送から一般ユーザーまで垣根なくデバイス間でやりとりが可能なプロトコルとしてIPの利便性を体感するには都合の良いプロトコルであると考えたため「IIJ Studio Tokyo」での主要プロトコルとして採用に至りました。

TV番組制作でもZoomやスマートフォンを利用し遠隔地から出演する場面では、IP映像を一旦SDIに変換し制作しているの

	SDI	SMPTE 2022	SMPTE_2110	NDI
圧縮	×	×	○	○ NDI Codec(DCT)/NDIHX
アルファチャンネル	×	×	○	○
HD(1080/59.94i) Data Rate	>1.5 Gbit/s	>1.5 Gbit/s	>1.5 Gbit/s	>100 Mbit/s
UHD(2160/60p) Data Rate	>12 Gbit/s	>12 Gbit/s	>12 Gbit/s	>400 Mbit/s

表-1 SDIとIP映像の比較

が現状ですが、IPのまま制作を行った方が効率的であるとも考えられます。しかしながらIPをメインに制作することは容易ではありません。数十年に渡りベースバンドで培ってきたノウハウや作法・安定性・オペレーションを刷新するには根気と時間、またあらゆる人員の理解が必要となります。

筆者は前職で10年近くの歳月を費やしてリニア編集からファイルベース編集への移行・定着までの変革業務（デモンストレーション、構築、アフターサービス）を行ってきましたので、「Live映像制作」におけるIP化も様々な苦労があると考えています。

3.5 将来の映像制作

将来的にはクラウド上に制作環境が構築され、SDIなど専用のインタフェースなしに映像をやり取りできる「Live映像制作」が可能になると考えます。しかし、すべてがクラウド上で完結するというよりは、クラウド上で行った方がメリットの多い部分が集中して管理されるようになり、「ポストプロダクション映像制作」環境との融合が進むと感じています。NDIは低CPUと1Gネットワークを用いてクラウド上で扱いやすいプロトコルで、内部処理には好都合かつ安価に映像のやり取りが可能と考えます（図-3）。

IIJ Stuido TOKYOでは、まずローカル環境に近い状態からIPベースの制作環境を整え、安定性やレイテンシーなどクラウド上でもボトルネックになってくるであろう課題に対して体験、体感しながら利用環境にマッチする「IT-Live映像制作」の取り組みを始めています。また、IIJが開設した白井データセンターキャンパスでは、ローカル5Gを用いた4k NDI伝送での画質、遅延量の体験なども行える研究拠点（白井ワイヤレスキャンパス）の運営を開始しており、他にも様々な取り組みを行ってきました。

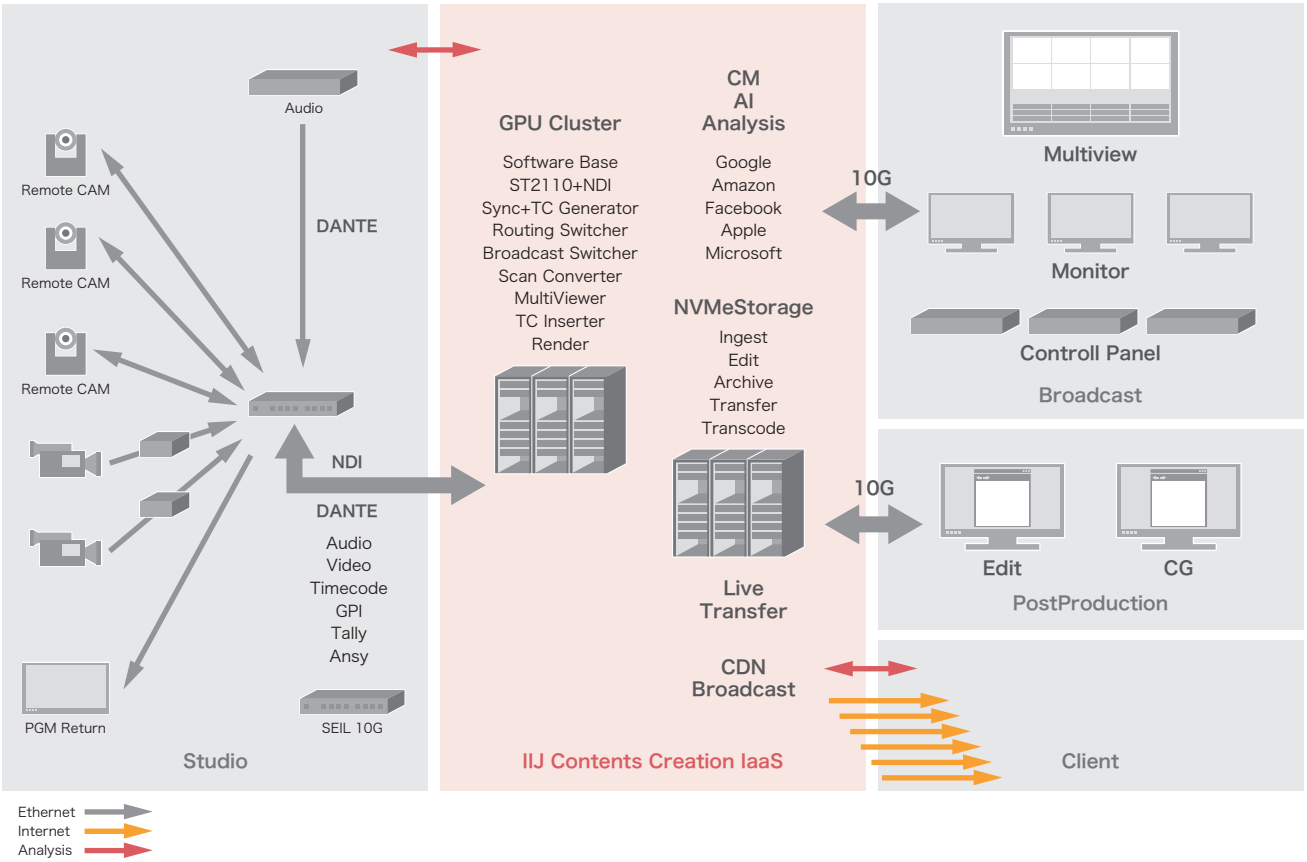


図-3 将来的なIT放送局の構想イメージ

3.6 過去の実績や取り組み

■ 2019年実績

ST2110非圧縮リモートプロダクションにおける放送局向けPoCに複数参加しました。各社メーカがそれぞれの放送機器を持ち込み規格の解釈や通信状況の確認を行いながら映像確認を行っており、多くの課題や情報を共有することができました。

■ 2020年実績

ローカル5Gを利用した4k NDI伝送デモ設備を白井データセンターキャンパスへ構築し以下のような特徴を体験いただける設備を公開しています。スタジアムや工場などリモートカメラの移動が頻繁な環境やセキュリティに課題を抱えている方にご覧いただきたい設備です。

写真-9:白井ワイヤレスキャンパス
ローカル5Gを用いて4kNDIの画質と低遅延性を実現

写真-10:パナソニックPTZリモートコントローラーと
リモートカメラの実機

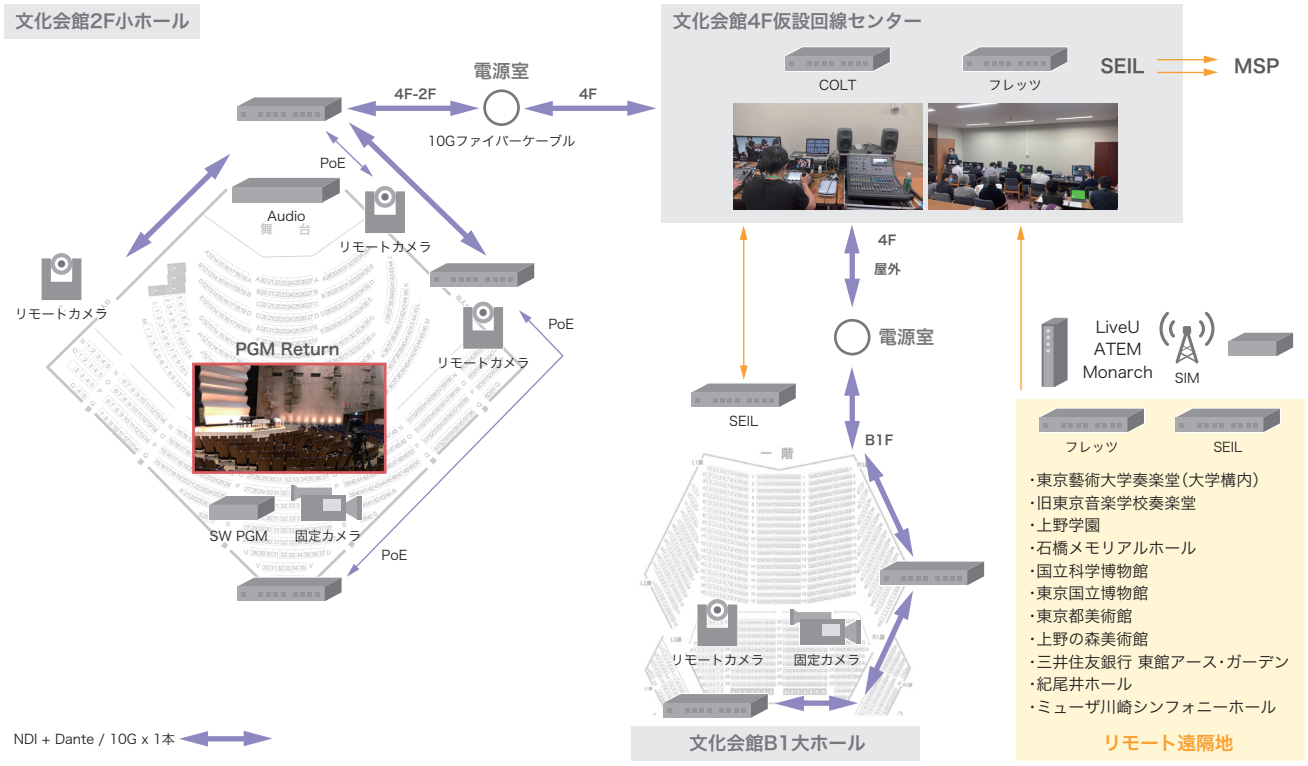


図-4 文化会館内でのネットワーク構成

・ 低遅延性・高画質性を体感可能な双方向なネットワーク
・ 免許周波数帯を用いるため通信品質が安定している
・ Wi-Fiに比べてセキュアかつ低遅延

■ 2021年実績

2021年の春祭では公演会場のひとつである文化会館内にNDIを利用したサブコントロールルームを仮設し、リモートプロダクション設備を構築し公演を配信しました。会場とサブコントロールルームはLANケーブルのみで接続し、リモートカメラ3式から伝送される映像・音声・タリー信号をケーブル1本で送受信可能なインフラを作り上げました。通常のベースバンドで同様に配線を行う場合はそれぞれの機器に専用のケーブルを配線する必要があるため、作業的な労力や接続ミスが発生しやすくなりますが、IPであれば配線のミスや作業負荷を容易に減らすことができます。ネットワークやカメラ機器も安定しており、NDIの画質や応答速度など含めて本番環境においても実用可能と判断、IIJ初のNDI実戦投入となりました。ただ、実際の現場では、会場を期間中全て押さえているわけではないため、電源やネットワーク線の配線と撤収を公演ごとに行わなければなりません。サーバ機器もほぼ毎日のようにシャットダウンさせる必要があり、動作確認の軽減など安定運用の観点から常設のサブコントロールルームの必要性を感じた最初の配信となりました。

■ 2022年実績

2022年の春祭ではSRT/H.265を利用した4会場同時リモートプロダクション配信を行いました。NDIと異なる点としてはレイテンシーが大きいため、SRTの接続モードを”コマ落ちするが応答性能が良い”「カメラ調整接続モード」と”バッファサイズを大きくし安定した伝送が可能な”「公演接続モード」の2種類を事前に設定し、本番前に瞬時に切り替えることで対応を行いました。会場からの映像は5秒の遅延で上野から飯田橋のエンコーダーに届くように調整し、安定した映像配信を行いました。

写真-11：PTZリモートカメラ

写真-12：PTZリモートカメラ（右）とL3VPNを構築させたSEIL（左）

写真-13：仮設サブコントロールルーム

3.7 「IIJ Studio TOKYO」構築時の苦労した点や工夫

これまでの様々な試みや経験から常設スタジオの必要性、有用性を認識し、常設のスタジオを構築することになりました。スタジオ稼働開始直後はTriCasterがクラッシュするなどの挙動も見られました。また、アップデート作業や設定変更、接続方法の変更など製品単体で手を加えなければならないといった製品の癖を知る必要がありましたが、現在では非常に安定した動作をしてくれています。またNDIの一部をマルチキャストに設定するなどしてネットワーク全体の帯域を有効利用するように設定を組み替えるなど細かな調整を行っています。また、メンテナンス性や対障害に対してはPCベースで構成されたTriCasterの起動イメージをフルバックアップし、大幅なシステムアップデートやシステム変更時には定期的にバックアップを行うことでトラブル時の早期リカバリーを可能にしています。また内部で作成したTriCasterのSessionデータはファイルサーバに同期させ随時バックアップを取り、万が一TriCasterが起動しなくなった場合にはTriCaster本体を交換することで即時復帰できるように定型化・文章化を行っています。特に重要となるのが手順書やトラブル時の対応情報は、社内で様々なツールを利用し日々情報の積み上げを行なっています。

3.8 後書

「夢物語のようなことが本当にできるのか？」先端技術を技術的な面からの「できる・できない」だけではなく、実際のオペレーションレベルまで落とし込み運用できるようにすることも重要です。専任のスタジオオペレータは20年も30年も専任で業務を行っているのでとにかく操作が早いです。ダイレクト感がなく応答性の悪いシステムは「使えない」と即判断されてしまう傾向にあり、どの程度の制作であれば耐えられるのか、どういった案件で特徴を活かせるのか見極めることも今後の方向性を決める上で大切なことであると考えます。

IIJのIPスタジオ「IIJ Studio TOKYO」はまだ始まったばかりですが、先端の技術を取り入れながら映像制作の基本を習得し、映像制作分野におけるIPの可能性や安定性の向上、管理、監視方法などの検証も行いながら技術革新を向上させています。既に、優秀なオペレータの入社やIIJエンジニアリングからの出向、また外部取材やコンサルタントの方の協力など、スタジオに共感いただける方々のコミュニティが始まっており、非常に良い流れが生まれています。

今後、IIJでは映像業界を含め様々な業界に対してもネットワークと人がつながる社会に貢献できる活動を進めてまいります。

執筆者：

角田 敦（すみた あつし）
IIJネットワーク本部 xSPシステムサービス部 配信ビジネス課。
前職では映像総合商社にてセールスエンジニアとしてポストプロダクションや放送局向けにノンリニア編集システムの導入やサポートに従事。2019年7月、IIJに入社。ST2110リモートプロダクションPoCなどに参加、オリンピック関連の配信や現時点での春祭配信システムにおける映像制作部分の基礎設計から運用までに携わり現在に至る。

「3-2 IIJ Studio TOKYO 設備の概要」担当
今西 亮太（いまにし りょうた）
IIJネットワーク本部 xSPシステムサービス部 配信ビジネス課。
2015年、IIJエンジニアリング入社と同時にIIJの配信事業に携わり、CDNサービスの運用・保守やイベントの収録・配信業務を担当。

IIJバックボーン30年間の変遷

4.1 はじめに

1993年、ルータ数台から始まったIIJバックボーンも今では数千台に及ぶネットワーク機器から成る大規模なネットワークへと進化してきました。その過程においては通信技術や経路制御技術、はたまたルータのハードウェア性能限界や電源事情等々、インターネットの急激な成長に追い付かず各種課題を抱えながらも、安定したインターネット環境を提供するため知恵と工夫により辛うじて乗り切ってきた日々であったように思います。

この章の前半では、IIJバックボーンがどのような経緯・理由でどのように変化してきたのか、またどのような工夫を加えたのか時代背景を交えつつ紹介していきたいと思います。また後半では、これまでにIIJが行ってきたネットワーク運用に係るセキュリティ対策を取り上げます。

4.2 IIJバックボーンの変遷

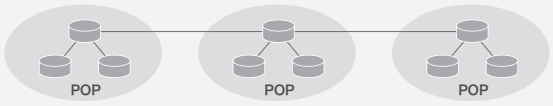
4.2.1 1993〜2002年 黎明期(リソース不足との戦い)

インターネットが学術利用から商用利用へと移り変わろうとしている頃は、まだまだインターネットに対する認知度が低く接続するための環境[*1]も十分に整っていない中で利用料金も高額[*2]であったことから、トライアル的な利用が主流でした。

■ 黎明期における物理構成の変遷

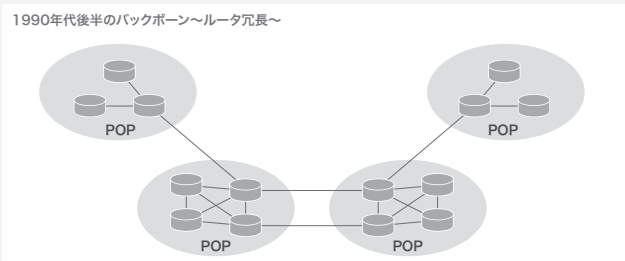
バックボーンはPOP(Point Of Presence)ごとに1台のバックボーンルータを設置し1本の専用線でPOP間を数珠つなぎに結ぶシングル構成から始まります。

シングル構成のまま拡張を続けたIIJバックボーンですが、1999年頃からインターネット上での金融取引が始まるなど、企業でもネット活用が一般化するにつれインターネット

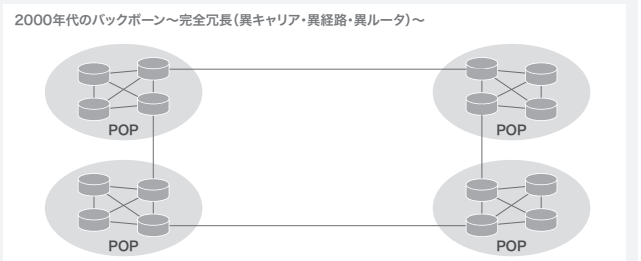


各POPにバックボーンルータ1台を配置し、バックボーンルータ間を1本の回線で接続する数珠つなぎ構成

図-1 初期のバックボーン



主要なPOPではバックボーンルータと回線の冗長化を開始。シングル構成とデュアル構成の混在時期



各POPにバックボーンルータ複数台を配置し、POP間の接続は異なる回線事業者の回線を利用。ファイバルートも異経路となるよう調整し、同時切断が発生しない構成へと進化

図-2 バックボーンの拡張

＊1　WindowsやMac にTCP/IP のスタックが標準搭載されたのは1995年頃。
＊2　45Mbpsの専用線接続におけるインターネット利用料が2000万円/月。

に求められる品質がより厳しくなり始め、耐障害性向上への取り組みが本格的にスタートします。まずは主要なPOPから回線及び機器の冗長化を開始し、2002年頃には完全冗長化を終えました。

【こぼれ話】

2002年冬、福岡POPにおいてバックボーン回線を2重化していたにも関わらず両回線が切断し孤立させてしまう障害を起こしてしまいます。原因は同一ファイバールートになっていた一部区間においてファイバーケーブルに侵入した水が凍り損傷させたというものでした。これを教訓にバックボーン回線の異ルート化を取り入れました。

黎明期における経路制御の変遷

経路制御に関しては初期の頃から変わらず、EGP(Exterior Gateway Protocol)にはBGP[*3]、IGP(Interior Gateway Protocol)にはOSPF(Open Shortest Path First)を利用しています。

また各ルーティングプロトコルで制御する経路の種別についても、顧客やプールアドレスなどユーザ利用ネットワークのルーティング情報はEGPで制御し、ネットワーク構成(機器や機器間のリンク)に関わるルーティング情報はIGPで制御するという点においても初期の頃から変わっていません。

IIJバックボーンにおける経路設計はEGPによってどこにネットワークが存在するかを伝搬させ、IGPによって目的のネットワークまでの通信経路を制御するという基本方針をもとに、シンプルだが堅牢なネットワークの実現を念頭にデザインされています。当初はルータ数もインターネット上の全経路数(フルルート)も少なく、BGPも発展途上にあったことから必要最低限の機能しか実装されておらず、iBGPの構成はフルメッシュで組む形態が基本でした(図-3)。

世の中にインターネットが認知され始めるとIIJバックボーンも拡張の一途をたどり、ルータ数も経路数も増加していきました。ネイバーの数が増え送受信するルーティング情報も増えてくるとメンテナンスや故障によるルータの再起動時にメモリが逼迫し、経路収束までに数十分を要したり再起動を繰り返すなど、安定性に欠く事象が現れ始めます。特にフルルートを日本国内の全ルータに送信する役割を担う海外ルータでは、遅延なども相まって限界を迎えていました。米国の現地で大変な思いをしながらメモリの調達と増設を行うと共に、ルーティング

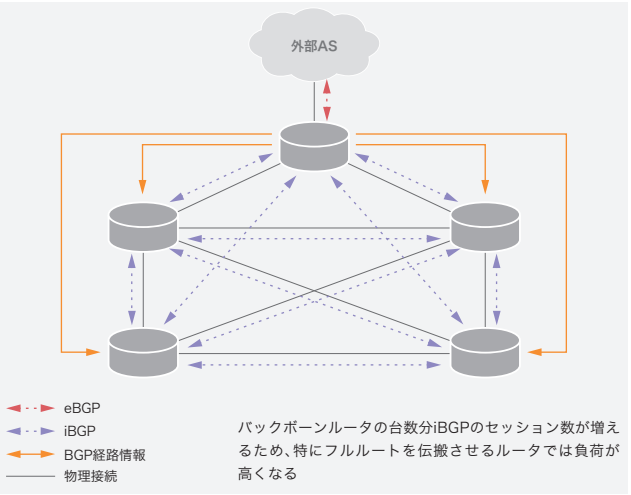


図-3 iBGPフルメッシュの例

*3 BGP(Border Gateway Protocol):初期はBGP3が主流でしたがCIDRの導入などによりBGP4(RFC1771)が誕生。βテストの頃よりBGP4を採用していました。

情報の送受信に伴う負荷を軽減することを目的に、BGPのルートリフレクション(RFC1966[*4])の導入に至ります。

最初に行ったのは東日本、西日本、及び海外の3クラスタ構成でした(図-4、5、6)。

2001年頃よりブロードバンド接続が普及しトラフィック量も大幅に増えるとIIJバックボーンも更に増強・拡張が進みます。すぐに限界を迎えるのは明白だったためクラスタの細分化を行いPOPごとにクラスタを設ける構成へと移行しました(図-7)。現在もこの構成がベースとなり15年以上経過します。

【こぼれ話】

当時、経路数の増加量は深刻な問題でした。シャーシ型のルータではモジュール式のI/Fカードでもメモリが逼迫寸前だったこともあり数百枚分に及ぶカードへのメモリ増設を深夜作業で実施し機能不全に陥る状況を回避していました。

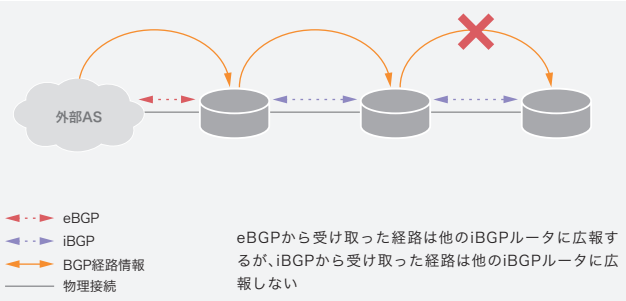


図-4 通常のBGP隣接関係図

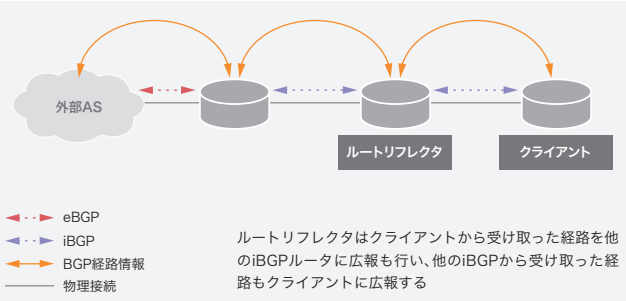


図-5 RR-RC隣接関係図

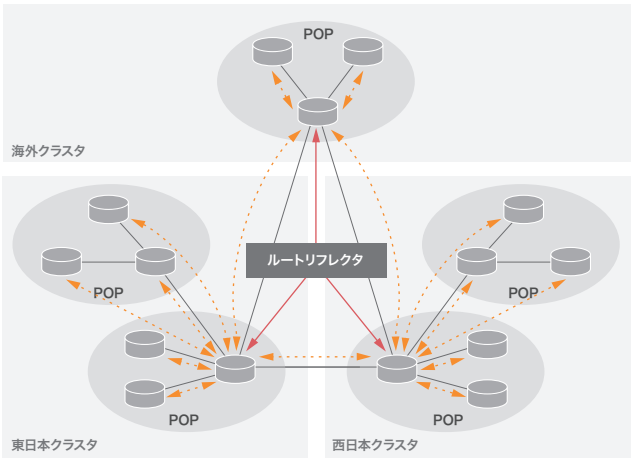


図-6 クラスタの概要図

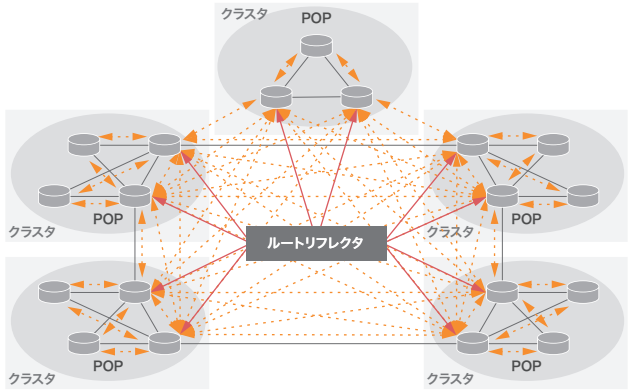


図-7 クラスタ細分化の概要図

*4 RFC1966 BGP Route Reflection An alternative to full mesh IBGP

【こぼれ話】

ルータのCPUが非力なため、OSPFのバックボーンエリアに存在可能な台数は50台程度と業界ではささやかれていました。これを受けIIJバックボーンにもOSPFのエリア分けを導入しますが、運用の難易度が飛躍的に高くなってしまい、事故も幾度か発生しました。幸いハードウェアの進化もありエリア分けは撤廃していますが、シンプルな構成が一番であると思わせる最たる例だと感じています。

様々な組織が管理・運営するネットワークの集合体であるインターネットでは、ミスオペレーションによる意図しない経路ハイジャックも稀に起こります。場合によってはインターネット全体に影響を及ぼすような事態にもなりかねず、他ASとのルーティング情報の送受信には細心の注意が必要です。IIJでは、IIJ自身も含め、ユーザが加害者にならないよう早い時期から全エッジルータで経路フィルタを導入していました。

初期はアクセスコントロールリストとAS-PATHフィルタの組み合わせにより制御を行っていましたが、新たなCIDRブロックやプロバイダ非依存アドレスなどの追加のたびに全エッジルータの経路フィルタを更新する必要があり、非常に煩雑で手間がかかっていました。そこでBGP Communities Attribute(RFC1997)の導入に踏み切ります。活用方法は至って簡単で、経路流入元や経路生成元でBGP communityを付加しバックボーン内部に伝搬させエッジルータでBGP communityを元に広報経路の制御を行うというものですが、経路制御が格段に容易になり設定変更箇所が大幅に減ることで安定運用にもつながりました。

以上のように黎明期においては各種技術も発展途上にありインターネットの成長速度に追い付かない状況の中、リソース不足との戦いでもあり試行錯誤をしながら基礎を固めていった時期になります。

4.2.2 2003〜2006年 普及期(品質向上とIPv6展開)

インターネットの利用が広がるにつれ、求められる品質も上がっていきました。2000年頃からバックボーンは順次冗長化されていき、長時間の断はほとんどなくなっていたものの、経路変化によるパケットロスが課題となりました。

インターネットにおける経路制御では、障害時に通信が自動的に迂回できるようにBGPやOSPFなどのダイナミックルーティング(動的経路制御)が利用されています。このダイナミックルーティングで、ネットワークの変化がルーティング情報としてネットワーク全体に伝搬され、それを受け取ったルータそれぞれが独自にルーティングテーブルを生成することで、ネットワーク全体が矛盾なく正常に通信できる状態を維持しています。この一連の動作による状態変化が収束(コンバージェンス)することをルーティングコンバージェンスと呼び、コンバージェンスに至るまでの時間(コンバージェンスタイム)がネットワークの品質性能を測る1つの要素となっています。

コンバージェンスに至るまでの状態変化は、大きく分けて以下のようなフェーズに分かれています。

- イベント検知(ルータの追加/削除、リンクのup/down、設定変更など)
- ルーティングプロトコルへの注入
- ルーティング情報の伝搬
- ルーティングの計算(ルーティングプロトコルごと)
- ルーティングテーブルへの反映

インターネット上では、メンテナンスや障害によって頻繁に状態変化が発生しています。状態変化が発生すると、コンバージェンスに至るまでの間、ルータ間でルーティングテーブルに矛盾が発生し、パケットロスが発生する可能性が出てきます。ネットワークが大規模になればなるほどコンバージェンス

タイムが大きくなりやすく、コンバージェンス性能がネットワーク品質に与える影響は大きくなります。よって、より安定した高品質なネットワークを作る上で、ルーティングコンバージェンスを高速化させることが非常に重要になります。

当時(2003年頃)はルーティングコンバージェンスを高速化する技術が登場し始めた頃でした。まずはIIJのバックボーン性能を調べてみようということになり、廃止予定の設備を利用して計測しました。機器のデバッグログと結果を突き合わせて、時間を要しているポイントを分析し、対策を検討しました。結果、大きく分けて以下の3つを実施しました。

- ルータのアップグレード
- 各種パラメータのチューニング
- Down検知しやすいトポロジに変更

ルータを最新のOSにアップグレードしないと、そもそも各種パラメータのチューニングができませんでした。バックボーンルータだけでも1年弱、すべてのルータが完了するのに数年を要しました。また、このアップグレードと併せてIPv6対応も実施していきました。アップグレードが完了したルータから順次パラメータをチューニングしつつ、デュアルスタック化していきました。また、当時はまだBFD(Bidirectional Forwarding Detection)が登場していなかったため、L2 Segmentを可能な限りPoint-to-Point構成に変更し、できるだけKeep Aliveに頼らないトポロジにするなど地道な対応なども進めました。その成果として、コンバージェンスタイムを1秒未満に実現しています。

そのほか、ルーティングコンバージェンス高速化の取り組みと並行して、品質を上げるための様々なシステム開発にも取り組みました。

- ルータのログから状態変化を監視するシステム
- ルーティングのアップデート情報を記録するシステム
- 拠点間のパケットロス・遅延を計測・監視するシステム

今となっては当たり前のような品質ですが、こうした取り組みにより、いち早く実現させていきました。

4.2.3 2007〜2010年 トラフィック格闘期(BF化)

増え続けるトラフィックに対して我々が利用しているルータの限界が見え、その当時の設計どおりにOC192(9.6G)の次の接続メディアとしてOC768(40G)の利用を検討しましたが、我々の要件に合うルータでOC768に対応しているのはCisco CRS-1しかありませんでした。しかし、床荷重が1tもあり設置できず早々に断念することになりました。そうなると、10GbEを複数本で増強するしかなく、ルータの10GbEポート数とキャパシティの問題からも設計を考え直さなければならない課題に直面しました。

そこで思いついたのが、CRS-1のバックプレーンの容量を増やすために使われていた3ステージスイッチファブリックのアーキテクチャを複数台のルータで実現し、巨大な仮想的な1台のルータ(以降ルータ群)にすることです(図-8-1)。

この構想ではスイッチファブリックに相当するバックボーンルータ(以降BFと略します)はエッジを担当するバックボーンルータ(以降BBと略します)すべてとつなぐ必要があります。しかし、逆から見るとBBルータ側はBFルータの台数分のポートが必要になりますが、エッジへの入出力を担当するためにすべてのポートをBFルータとの接続に使うわけにはいきません。このルータ群のキャパシティが4年間毎年2倍(現在のトラフィックの16倍)に増えても耐えられるだけのキャパシティを仮定として置き、BBルータの最大ポート数からBFルータへの接続用のポート数を算出して設計しました。

接続ポート数を解決した次には、複数台のルータで実現していることを逆手にとって、1ヵ所にしなくても複数拠点に分散して実現することで全体の台数を削減できることを思いつき、東京ではトラフィックが多かった拠点の3ヵ所をBFルータの設置場所に分散配置することを検討しました(図-8-2)。分散配置することで課題となるのが、拠点間の10Gの回線数が非常にたくさん必要になることです。当時の10GbEの回線単価を考えると非常に高価になることが想定され、分散配置しない方が安価になります。そこで、通信キャリアに想定している本数と共に1本あたりの回線単価がどれくらいになるのかを確認しつつ、自分たちで本格的に伝送装置を運用する場合の1本あたりの回線単価を比較して、一部の区間においては

自分たちで伝送装置を持つことにしました。簡易的な伝送装置は利用していたものの、本格的な伝送装置を利用するには敷居も値段も高かったのですが、何度もメーカに押しかけて試験をさせてもらったり、何度も説明を受けたり、伺っているうちに、我々の本気度を感じ取ってくれたあるメーカさんが、我々の想定している金額感に合わせてくれたのが導入の決め手のひとつとなりました。

分散配置の回線の問題が解決した次に、このルータ群と各拠点との回線の設計に入りました。今までの回線設計である1+1冗長では非常に多くの回線が必要となるためN+1冗長にしてコスト削減を検討しますが、奇数本数になるときの分散させる方法が非常に難しく、良い方法が見つかりませんでした(図-8-3)。結局3ステージファブリック構想は一部諦めて、東阪など主要拠点間はBFルータ同士をつなぐことでN+1冗長とすることにしました。BFルータ間で接続したために、BBルータから入ってきたトラフィックがどの東阪の回線を使ってどれくらい流れているかなどを明確にしなければ、障害やメンテナンス時のトラフィックの迂回や増強計画が立てられないという非常に難しい問題を生むことになります。この問題を解決するにはnetflowによる解析しかなく、解析に時間がかかってしまうと万一突発的なトラフィックが発生したときに対応できません。丁度、このときに分散システムによって高速な解析ができるシステムを独自開発[*5]していたことによって、障害やメンテナンスによる輻輳を発生させることがありませんでした。結局、4年耐えられる設計としていましたが、倍の8年間設計を変えることなく増強し続けることができました。

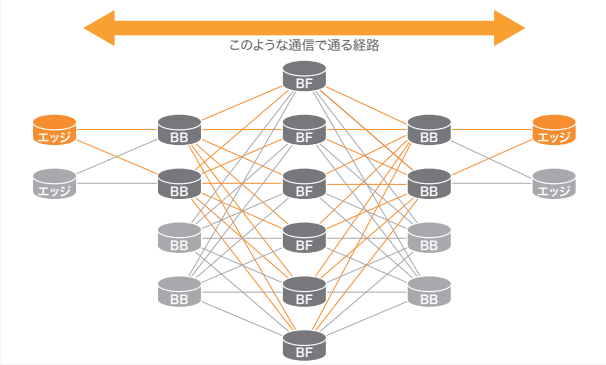


図-8-1:巨大な仮想敵な1台のルータ

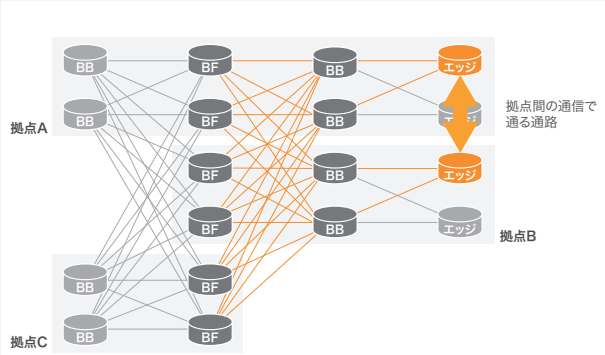


図-8-2:BFルータの分散配置

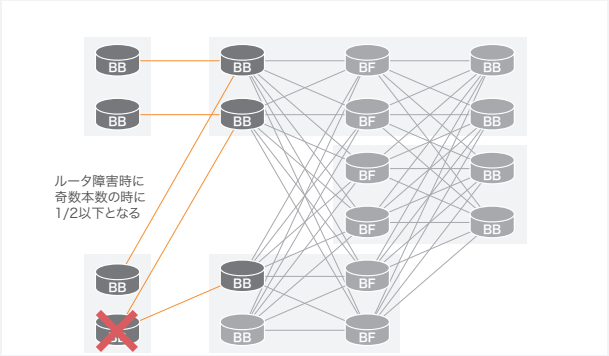


図-8-3:奇数本数になるときの問題

図-8 ファブリック構成のインターネットバックボーン 概要図

*5 IIR Vol.4、3章 クラウドコンピューティングテクノロジー「分散システムdddの実装と活用」(https://www.iij.ad.jp/dev/report/iir/004.html)を参照のこと。

4.2.4 2011年～ネットワーククラウド（統合コアの構築と閉域の拡充）

この頃になると既にAWSやGCP、Azureなど、そしてIIJでも「IIJ GIO」としてクラウドサービスを開始しており、クラウドサービスが本格化していきます。それに伴いインターネットトラフィックとは隔離された閉域の拠点間通信の需要が大きくなり、インターネットバックボーンとは別にプライベートバックボーンとしてMPLS/L3VPNを利用して拠点展開していくことになります。

インターネットバックボーンは前述のファブリック構成をとっており、ファブリックルータをスケールアウトさせることで全体のトラフィックを運ぶことができる構成でしたが、10Gメディアしかなかったため、トラフィックが増大してくるにつれて運用上の課題も多く抱えるようになってきます。POP内の接続についてはリンクを束ねるLAG（Link Aggregation）やIGP・BGP multipathなどのロードバランスを駆使することになるのですが、トラフィックフローのハッシュ値による分散では綺麗に分散するには限界があり、余計にポートを消費するようにもなってきます。また、どのリンクにIPパケットが流れているか分からないため正常性の確認が難しく、100Gで集約することを待ち望んでいました。

実際に100Gを実利用し始めたのは2012年頃で、JPNAPに100Gで接続を開始しています。既にインターネットバックボーンとしては東名阪で耐障害性を考えて異キャリア・異ルート・異拠点間の区間でOC192を20本程度利用していました。この構成から単純に100G化するにはコストもかかり過ぎてしまうため、100Gというキャパシティの利を活かして、ルート・拠点分散の冗長性を落とすことなく、以下のような点も一緒に実現することにしました。

- バックボーンネットワークの拠点回線の統合
- 東京・大阪依存構成の解消

IIJは自前でファイバーを持っていないため、長距離区間はキャリア回線を調達する必要があったため、複数のネットワーク面ごとにキャリア回線を個別に用意しなくてもよいようにMPLS/L2VPNでPW（Pseudo-Wire）を利用できるようにして、回線帯域を複数のネットワーク面でシェアできるようにしました。また、ルート・拠点分散の冗長性を各ネットワークで維持していくことは運用の手間が増える上にコストもかかるため、L2VPNがルート分散やトラフィックエンジニアリングの多くの部分を担い、MPLSの高速迂回によって回線障害などで発生するトポロジ変化を隠蔽することで、各ネットワークはよ

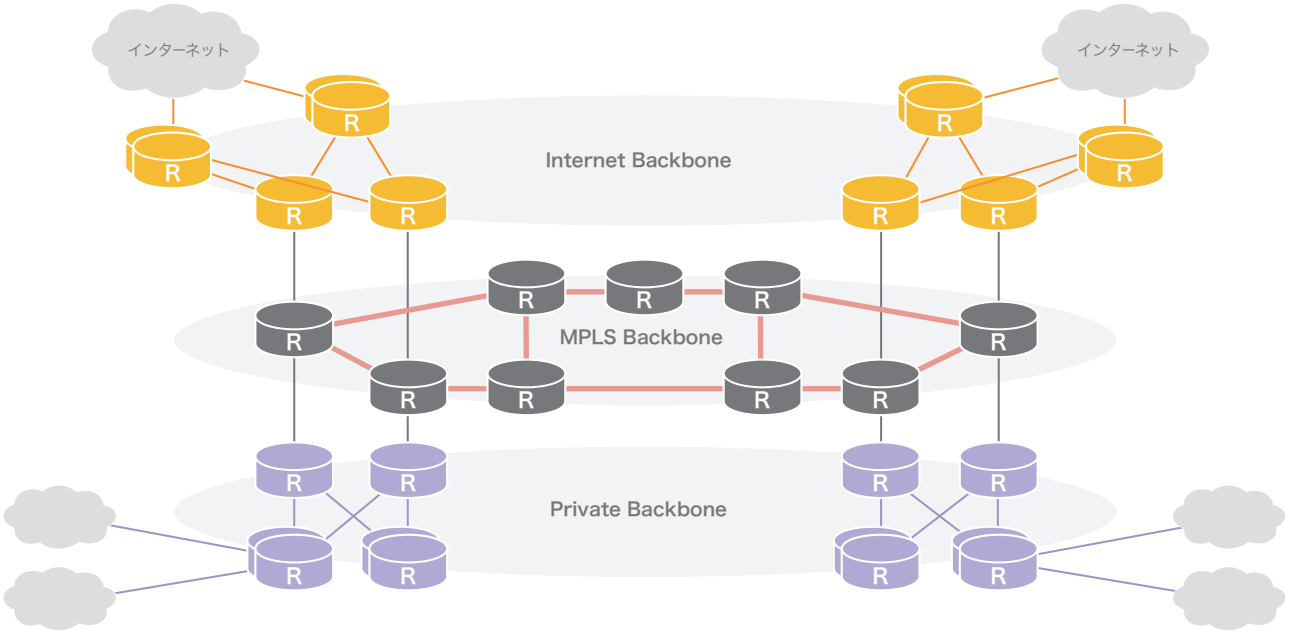


図-9 100G コアバックボーン概要図

り制御しやすい構成にすることにしました。トラフィックが多いインターネットバックボーンにおいては、コアPOP間をフルメッシュで結ぶことでコア拠点間のトランジットトラフィックをなくしてシンプルな構成にシフトしました。

東京・大阪依存構成の解消以前のバックボーンは東京や大阪近郊ではない拠点でも東京か大阪にぶら下がっている構成となっていました。トラフィックの効率性を考えるとその構成で十分でしたが、東京や大阪が被災した際にぶら下がっている拠点も通信ができない状況に陥ってしまうことになります。これを解消するべく札幌・仙台を関東非経由で名古屋へ岡山・広島・福岡・松江などを大阪非経由で名古屋に回線を延伸、日米間の国際線も東京・大阪・名古屋に分散配置して耐障害性を上げることを、数年かけて実施しています。

IIJのネットワークはもともとインターネットトラフィックの交換の中心であった米国にのみ拠点を持っていましたが、こうした取り組みと共に米国以外の地域にもネットワーク延伸しています。2013年にはヨーロッパ、2014年には香港とシンガポールにも延伸し、海外との接続性を米国のみに頼っていた構成からアジア・ヨーロッパ各地でダイレクトにトラフィック交換ができるようにもなり、インターネットの接続性も向上しています。

こうした100Gの統合バックボーンを導入することでインターネットトラフィックと比べて小さかった閉域のプライベートバックボーンの拡充もスムーズに行うことができ、パブリッククラウドとの相互接続もクラウドエクスチェンジとして順次拡充しており、昨今の急速なワークスタイルの多様化するニーズにも対応できるようなネットワーククラウドとして拡張を実施してきました。

以上、黎明期から順に説明してきたとおり、IIJバックボーンもその時代の課題を解決してきたことで改善を繰り返し、変化してきました。社会インフラとして欠かせないインターネットは今後もより高い信頼性が求められるモノになっていくことでしょう。IIJはこれからもこうした社会のニーズに応えていくための信頼できる社会インフラとして拡張を実施していきます。

4.3 IIJ ネットワークのセキュリティ対策

IIJはネットワークが適切に利用可能であるようにセキュリティの向上にも取り組んできました。ここでは、ネットワーク運用に関わるセキュリティ対策のうち、IIJで実施した取り組みをいくつか紹介します。

4.3.1 Source Address Validation(送信元検証)

インターネットでは基本的にIPパケットヘッダの宛先IPアドレスを頼りに経路情報を探索し、IPパケットを宛先に届けています。IPパケットヘッダには送信元IPアドレスの情報もありますが、これが間違っていても宛先にはIPパケットが届きます。IPパケットを受け取った宛先はIPパケットヘッダの送信元IPアドレスを見て通信元を判別し、必要に応じて応答パケットを送出します。送信元IPアドレスが間違っていた場合、間違ったIPアドレスの情報を信じて、全く見当違いのホストに応答パケットが送出されることになります。この挙動は悪意ある攻撃者に悪用されるようになりました。例えば、攻撃元を識別しづらくしたり、他のホストに偽装して既存の通信を乗っ取ったり、特定ホストに応答パケットを送付させたりする攻撃手法が考案され、実際に攻撃で使用されました。

2005年頃からDNSを悪用したDNSリフレクター攻撃(DNS増幅攻撃)が観測されるようになりました。この攻撃は送信元IPアドレスを攻撃対象ホストのIPアドレスに偽装して、踏み台となるネームサーバにDNS問い合わせを送信します。名前解決でデータ量が増えた応答をネームサーバから攻撃対象ホストへ送付させることで、攻撃対象の帯域を効率的に埋め尽くし、サービス不能を狙う攻撃です。攻撃者は事前にインターネットに接続されたホストを乗っ取り、そうしたホストから送信元IPアドレスを偽装したパケットを送出することで攻撃を

実施していました。IIJではこうした状況を鑑み、IIJの接続サービスが攻撃に悪用されないように、送信元IPアドレス偽装を防ぐ技術の導入を進めることとしました。

IPアドレスの偽装に関する問題は早くから認知されており、RFC 2827（BCP38）やRFC3704（BCP84）として問題と対策が文章にまとまっています。対策には、できるだけ接続サービスを終端している箇所の近くで、適切な送信元IPアドレスが用いられているかどうかを検証する必要があります。当時IIJで利用していた機器では送信元IPアドレスを検証するために、経路探索の仕組みを応用したunicast Reverse Path Forwarding（uRPF）と、パケットフィルタリングの機能を用いるAccess Control List（ACL）が利用可能でした。機種やソフトウェアのバーションによっては機能に制限があったので、機種に応じて適切な方法で実装することにしました。2006年3月には送信元検証をすべての接続サービスに導入する旨アナウンス[*6]し、順次適用を完了しました。これにより、IIJの接続サービスが攻撃に悪用されることを防ぎ、ネットワーク全体のセキュリティ向上と安定した運用を実現しました。

4.3.2 Internet Routing Registry（IRR）

インターネットに様々なネットワークが接続し、拡大する中で、ネットワーク間でBGP経路制御のポリシー調整をどう実現するかは大きな課題です。これに対し、IRRは各ネットワークが経路制御ポリシーをオブジェクトとして登録し、お互いにそれぞれのポリシーを参照できる機能を提供しています。IRRに登録されたオブジェクトは、経路フィルタの自動生成や障害発生時の確認用などに利用されています。IIJではroute、route6、as-setなどIRRの活用でよく参照されている主要なオブジェクトを登録し、情報が常に最新状態になるよう維持しています。更に、オブジェクトを登録するIRRサービスとして1990年台からMeritが運用するMerit RADbを利用してきました。2005年からはJPNICの運用するJPIRRも併用して、現在は主にこれら2つのIRRを利用しています。

IRRに登録されているオブジェクトが勝手に書き換えられてしまうと、それを参照した他のネットワークで間違った経路フィルタが生成されるなどして、IIJの到達性に問題が生じるかも知れません。Merit RADbもJPIRRも基本的には電子メールを管理システム宛てに送信することで、オブジェクトの更新を行います。その際に利用できる認証方式にはいくつか選択肢があり、IIJではその中で一番強固なPretty Good Privacy（PGP）を利用した認証を利用することにしました。これはPGPの電子署名とその検証を利用した認証で、事前にオブジェクト変更権限を持つPGP公開鍵をIRRに登録することで利用できます。IIJでは2003年にPGP認証へと移行完了しています。

4.3.3 Resource Public Key Infrastructure（RPKI）

RPKIはIPアドレスやAS番号など、番号資源の分配を証明するPKIで、これを活用することで経路制御の安全性向上を実現することもできます。IPアドレスの分配を受けた組織は、そのネットワークをどのASから広報するかを、Route Origination Authorization（ROA）としてRPKIシステムから発行できます。この情報を用いると、BGPで受信した経路情報が妥当な広報元ASで生成されたものかを確認できるようになります。現状ではIRRの方が広く利用されていますが、RPKIの方が自動化に優れ、より信頼度の高い情報を利用できるため、今後RPKIの利用も広がるものと考えています。

IIJでは2020年に基本的なROAの発行を完了しています。ROAには経路の分割広報をどこまで許容するかを示す最大経路長が含まれますが、IIJでは分割広報しないので、広報経路の経路長をそのまま設定しています。これはRFC 9319（BCP185）でも推奨されている設定です。また、同じく2020年からピアとアップストリームから受信するBGP経路広告をROAの情報を用いて検証し、ROAと矛盾する経路情報を破棄するポリシーを導入しています。これにより、ROAを発行しているネットワークが間違った広報元ASから経路広告されてもIIJネットワークでは該当経路を判別して破棄することが可

＊6　IIJ、全接続サービスで「Source Address Validation（送信元検証）」を導入（https://www.iij.ad.jp/news/pressrelease/2006/pdf/0308.pdf）。

能となっています。また、Merit RADbではROAと矛盾するオブジェクトを自動的に削除する機能が実装されているため、ROAを発行することでIRRに間違ったオブジェクトを登録されないようにする防御手段にもつながっています。

4.3.4 Mutually Agreed Norms for Routing Security (MANRS)

インターネット運用におけるネットワークのセキュリティ対策は、多くのネットワークが協調的に導入することでその有用性が高まります。対策の導入を推進するためのグローバルな自主的活動として、MANRSが挙げられます。これはInternet Society(ISOC)の協力のもと、推奨されるセキュリティ対策を分野別に設定し、インターネット運用に関わる各組織に取り組みの実践を求めるものです。活動に賛同する組織はMANRSに自身の実践している取り組みを示し、参加することができます。

IIJでは、利用可能なセキュリティ対策を適宜導入してきました。これらはMARNSの推奨する実践とも合致しており、IIJは日本初の参加組織として2015年にMANRSに参加しました[*7]。IIJでは、今後ともインターネットの安定運用のために運用を見直し、継続的な改善を続けてまいります。

執筆者:

1993〜2002年 黎明期(リソース不足との戦い)
岩崎 敏雄(いわさき としお)
IIJ 基盤エンジニアリング本部 運用技術部長

2003〜2006年 普及期(品質向上とIPv6展開)
淺野 善男(あさの よしお)
IIJ ネットワーク本部 インフラ技術部

2007〜2010年 トラフィック格闘期(BF化)
片岡 邦夫(かたおか くにお)
IIJ 基盤エンジニアリング本部

2011年〜 ネットワーククラウド(BBコアフルメッシュ化、閉域の拡充)
津辻 文亮(つつじ ふみあき)
IIJ 基盤エンジニアリング本部 ネットワーク技術部

IIJネットワークのセキュリティ対策
松崎 吉伸(まつざき よしのぶ)
IIJ 基盤エンジニアリング本部 運用技術部 技術開発課

＊7　MANRS Turns 1 and First Japanese Operator, IIJ, Joins(https://www.manrs.org/2015/11/manrs-turns-1-and-first-japanese-operator-iij-joins/)。

Information

IIJ Engineers Blog 最新トピック

IIJのエンジニアブログで昨年12月1日から24日まで実施したアドベントカレンダー。全24記事の中からぜひ読んでもらいたい、編集長の堂前オススメ記事を紹介します。
IIJ 2022 TECHアドベントカレンダー（https://eng-blog.iij.ad.jp/adventcalendar2022）。

1

みんな大好き自宅DIYネタ

自宅でLAN工事してみた

高畑 雅弘

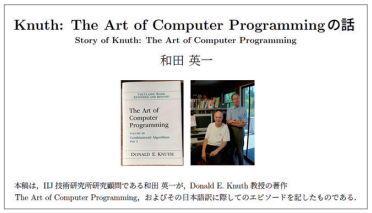
今回のアドベントカレンダーの中でアクセス数一位でした。

この記事のURL（https://eng-blog.iij.ad.jp/archives/16908）。

2

和田先生ならではの記事

Knuth：The Art of Computer Programmingの話



和田 英一

Knuth教授の著書「The Art of Computer Programming」の名前をご存じの方は少なくないと思いますが、通読された方は多くないかもしれません。同書の日本語翻訳者でもありIIJ技術研究所顧問でもある和田英一が、ズバリ書いています。

この記事のURL（https://eng-blog.iij.ad.jp/archives/16094）。

3

私も5分で動かせました

マルウェア解析に役立つ、実行ファイルのケーパビリティ検知ツールcapaの入門

ちひろ

マルウェアの解析というと非常に高度な技術という印象がありましたが、この記事で紹介しているcapaは、そのとっかかりとしてとても面白いツールです。手元のPC上でそのまま実行するだけでexeファイルの素性がなんとなく分かります。是非お試しください。

この記事のURL（https://eng-blog.iij.ad.jp/archives/15926）。

4

人は物理から離れては生きられないのよ

ケーブルシップをたずねて三千里

竹﨑 友哉

各所の「通信インフラ」を訪ね歩いている竹﨑のレポート、最新作です。私たちもお世話になっている海底ケーブルを「敷設する船」を（外から）見学した様子を寄稿してくれました。竹﨑のこれまでのインフラ歩き記事も一緒にご覧ください。

この記事のURL（https://eng-blog.iij.ad.jp/archives/16829）。

5

スクラムはソフトウェア開発だけはない

スクラム導入を巡る冒険　〜インフラチームの場合〜

m-t-a-n-a-k-a

開発と運用という異なる時間軸で動く業務にどうやって1つのチームで取り組むのか。そんな課題に、IIJのIaaSの設計・構築及び運用を一手に引き受けるチームがスクラムで挑んだというお話です。

この記事のURL（https://eng-blog.iij.ad.jp/archives/15661）。

6

皆さんのインターネットはどこから？

「My First Internet」シリーズ

IIJにも様々な世代のエンジニアがいます。インターネットの黎明期から関わっている世代だけでなく、物心ついたときにはすでにインターネットが当たり前になっていたという世代も。共通テーマ「あなたが最初に触れたインターネットは？」で記事を書いてもらいました。

この記事のURL（https://eng-blog.iij.ad.jp/archives/17199）。

March 2023 Vol.58

IIJ
Internet Initiative Japan

株式会社インターネットイニシアティブ(IIJ)について

IIJは、1992年、インターネットの研究開発活動に関わっていた技術者が中心となり、日本でインターネットを本格的に普及させようという構想を持って設立されました。
現在は、国内最大級のインターネットバックボーンを運用し、インターネットの基盤を担うと共に、官公庁や金融機関をはじめとしたハイエンドのビジネスユーザに、インターネット接続やシステムインテグレーション、アウトソーシングサービスなど、高品質なシステム環境をトータルに提供しています。
また、サービス開発やインターネットバックボーンの運用を通して蓄積した知見を積極的に発信し、社会基盤としてのインターネットの発展に尽力しています。

本冊子の情報は2023年3月時点のものです。

IIJ-MKTG019-0058

株式会社インターネットイニシアティブ
〒102−0071 東京都千代田区富士見2-10-2　飯田橋グラン・ブルーム
E-mail：info@iij.ad.jp　URL：https://www.iij.ad.jp